У телекома рейтинг позитивный

Летние котировки ряда компаний телекоммуникационного сектора поддержала информация от международного рейтингового агентства Fitch Ratings, которое подтвердило долгосрочные рейтинги дефолта эмитента шести МРК на уровне «BB» и изменило прогноз для них со «Стабильного» на «Позитивный».

Анна ЗАЙЦЕВА,
аналитик
УК «Финам Менеджмент»

Изменения коснулись ОАО «Центр-Телеком», ОАО «Северо-Западный Телеком», ОАО «Волгателеком», ОАО «Сибирьтелеком», ОАО «Уралсвязьинформ» и ОАО «Дальсвязь». Следует отметить, что большинство компаний сектора опубликовали позитивные результаты по РСБУ за II квартал и I полугодие 2010 г., а также исполнили обязательства по выплате дивидендов по итогам прошлого года.

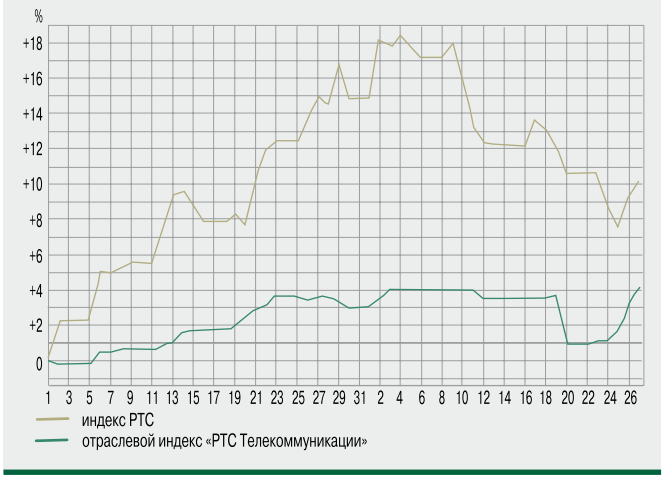
За два летних месяца, с 1 июля по 27 августа, отечественный фондовый рынок в целом продемонстрировал умеренный прирост капитализации. Причем если в июле публикации позитивной макроэкономической статистики из ЕС и США и сильная квартальная отчетность ряда крупнейших эмитентов помогли скомпенсировать понесенные на торгах в мае-июне потери, то в августе на российский рынок акций вновь вернулась коррекция. Ее причинами стали как сезонное снижение активности на фондовых площадках, так и усилившиеся опасения инвесторов относительно перспектив мировой экономики, подкрепленные противоречивыми данными об американской экономике и возможным сокращением объемов поддержки сегмента рискованных активов со стороны мировых финансовых регуляторов. Всего за рассматриваемый период индекс ММВБ прибавил 4,37%, до 1366,50 пт, а индекс РТС – 6,12%, до отметки 1421,47 пт. В то же время отраслевые индексы «ММВБ телекоммуникации» и «РТС Телекоммуникации» выросли на 4,79% (2053,88 пт) и 2,27% (205,75 пт) соответственно.

За рассматриваемый период обыкновенные акции «Ростелекома» потеряли символические 0,01%, снизившись в цене до отметки 109,79 руб. Компания опубликовала в целом негативную отчетность по РСБУ за I полугодие 2010 г. Ее чистая прибыль составила 2233,9 млн руб., на 5,5% меньше по сравнению с аналогичным показателем I полугодия 2009 г. Выручка «Ростелекома» за первое полугодие текущего года составила 28 467,7 млн руб., сократившись на 6,8% по сравнению с аналогичным периодом 2009 г., что стало следствием снижения доходов в ряде традиционных сегментов. Помимо этого, «Ростелеком» подписал новый договор о межоператорском взаимодействии с «Синтеррой», в соответствии с которым стороны будут предоставлять друг другу каналы связи и оптические волокна на взаимовыгодной основе.

Акции «Сибирьтелекома» подорожали на 5,35%, достигнув цены в 1,9090 руб. Компания выплатила дивиденды по привилегированным акциям за 2009 г. в размере 213,188 млн руб. Общий же размер дивидендов, начисленных на «префы», составил 230,303 млн руб.; таким образом, компания выплатила 92,6% от этой суммы. Среди важнейших событий лета следует выделить и избрание советом директоров «Сибирьтелекома» нового состава правления.

Капитализация «ЦентрТелекома» возросла на 5%, до уровня 23,1 руб. за акцию. Чистая прибыль оператора, со-

Динамика индексов и инструментов РТС



гласно отчетности РСБУ, увеличилась во II квартале 2010 г. на 32,98% – до 1 953,099 млн руб., а по итогам первого полугодия достигла 3422 млн руб., что на 36,9% превышает аналогичный показатель прошлого года.

Бумаги «Дальсвязи» подорожали на 6,73% до отметки 96,84 руб. По данным РСБУ, во II квартале компания получила чистую прибыль в размере 704,510 млн руб., что на 39% превышает аналогичный показатель I квартала (506,186 млн руб.). Увеличение прибыли связано с получением дивидендов за 2009 г. от дочерней компании ОАО «Сахателеком». Таким образом, «Дальсвязь» в I полугодии получила чистую прибыль в размере 1210,696 млн рублей против 1071,720 млн руб. в аналогичный период 2009 г.

Котировки акций «Северо-Западного Телекома» прибавили 9,15% до уровня 22 руб. Из корпоративных новостей стоит отметить утверждение советом директоров компании нового состава правления. Чистая прибыль оператора по РСБУ увеличилась по итогам I полугодия до 2,3 млрд руб.

За рассматриваемый период бумаги «Уралсвязьинформа» выросли на 7,31%, достигнув цены 1,0420 руб. Компания выполнила обязательства по выплате дивидендов за 2009 г. по привилегированным акциям в объеме 406,757 млн руб., что составило 99,966% общего объема выплат. Чистая прибыль «Уралсвязьинформа» в I полугодии 2010 г. увеличилась в 2,1 раза – до 3977,2 млн руб., отношение чистой прибыли к выручке выросло на 9,1 процентного пункта – до 18,6%. Показатель EBITDA составил 9490,2 млн руб. (прирост 23,7%), отношение EBITDA к выручке увеличилось на 6,3 процентных пункта, достигнув по итогам I полугодия 44,5%.

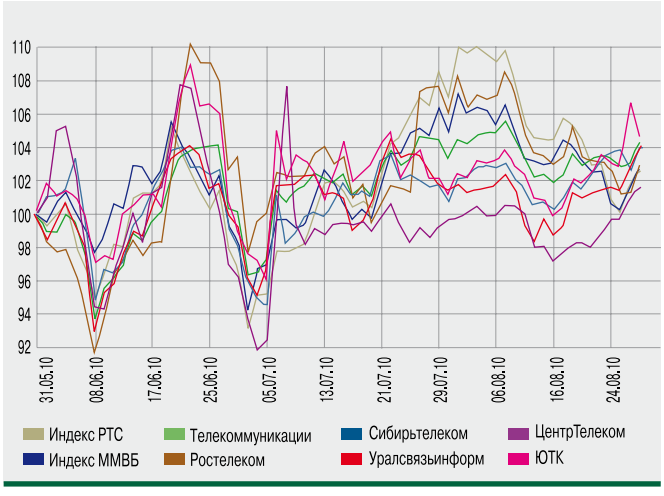
Снижение в сегменте МРК в июле-августе продемонстрировали лишь акции «Волгателекома», которые подешевели на 0,96% до отметки 100,25 руб. Возможно, незначительная коррекция была обусловлена некоторой «перекупленностью» бумаг оператора, поскольку его отчетность за II квартал 2010 г. по РСБУ выглядела вполне позитивно. Так, чистая прибыль ОАО «Волгателеком» по итогам полугодия выросла на 25,9% до 2803,5 млн руб., а выручка компании продемонстрировала прирост в 5,6%, достигнув отметки 14 121,5 млн руб. По сути отчетность «Волгателекома» за I полугодие по РСБУ – одна из лучших среди МРК; компания показывает весьма высокие результаты по эффективности. Кроме того, за квартал значительно выросли доходы от предоставления услуг ШПД. Оператор также выплатил дивиденды по привилегированным акциям за 2009 г., общая сумма которых достигла 403,35 млн руб.

Большинство компаний сектора опубликовали позитивные результаты по РСБУ, а также исполнили обязательства по выплате дивидендов по итогам прошлого года

Позитивная динамика наблюдалась и в мобильном сегменте. В частности, акции сотового оператора МТС подорожали на 6,74% – до отметки 248 руб. Компания опубликовала хорошие результаты за II квартал и I полугодие текущего года. Квартальная консолидированная выручка выросла на 16,5% (год к году) и достигла $2,77 млрд. Выручка за первые 6 месяцев 2010 г. продемонстрировала рост на 19,4%, до уровня $5,39 млрд. Основным фактором роста стало увеличение абонентской базы оператора, размер которой на конец июня 2010 г. достиг 103,41 млн человек (+1% к уровню годичной давности). При этом чистая прибыль группы выросла на 40,9%, до $734 млн. За рассматриваемый период МТС совершил ряд крупных сделок: приобрел у кипрской компании Cavolo Trading Limited 100% акционерного капитала группы компаний ЗАО «Мультирегион» за $123,5 млн, а также 95% акционерного капитала ОАО «Метро-Телеком» у ЗАО «Инвест-Связь». Сумма сделки составила 339,35 млн руб. (или $11,01 млн).

Капитализация АФК «Система» в июле-августе снизилась на 0,96% – до уровня 25,69 руб. за акцию. Пожалуй, ключевым событием стало приобретение компанией 51% акций ООО «М2М телематика». Помимо этого, «Система» опубликовала и неплохую отчетность по РСБУ, согласно которой в I полугодии 2010 г. компания получила 44,99 млрд руб. чистой прибыли против убытка в 9,8 млрд руб. годом ранее. Возможно, инвесторов порадовал и тот факт, что рейтинговая служба Standard&Poor's пересмотрела прогноз по рейтингам компании с «Негативного» на «Стабильный» и подтвердила ее долгосрочный кредитный рейтинг на уровне «BB». ИКС

Динамика индексов РТС и телекоммуникационных компаний в период с 31 мая 2010 г. по 24 августа 2010 г.



Окончание. Начало см. в «ИКС» № 7-8'2010

Камо грядеши, закон?

Федеральный закон с порядковым номером 152 породил проблемы не только правовые, о которых говорилось в прошлой публикации. Его влияние гораздо шире и простирается в сферы технические и даже государственные.

Михаил ЕМЕЛЬЯННИКОВ, директор по развитию бизнеса НИП «Информзащита»

Проблемы технические

При определении и реализации защитных мер по охране конфиденциальности персональных данных в информационной системе законодатели пошли по технологическому пути создания обязательных для выполнения требований и системы контроля и надзора за их выполнением. Путь в принципе возможный, но, как оказалось, весьма сложный с точки зрения реализации и очень затратный. Альтернативой ему могло бы быть установление обязанности оператора обеспечивать конфиденциальность и значительное усиление ответственности за инциденты с персональными данными, наносящие ущерб их субъектам. Сама степень ответственности должна в этом случае стимулировать оператора принимать достаточные для избежания инцидентов меры, но выбор их и конкретных средств защиты ложатся целиком на оператора. Таким путем идет практически весь остальной мир. В помощь тем, кто плохо представляет себе, как построить систему защиты, разрабатываются методические документы, носящие, естественно, не обязательный, а рекомендательный характер. Примерами таких документов являются стандарты NIST «Special Publication 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)» и BS 10012:2009 «Data protection. Specification for a personal information management system». Следовать им или нет, решает оператор.

Мы пошли другим путем, что породило ряд очевидных проблем.

Определение значимости последствий нарушений безопасности при обработке персональных данных в зависимости от формально определяемого класса информационной системы представляется весьма спорным. Если следовать логике регуляторов, утечка номера моего сотового телефона из базы оператора связи (у оператора, имеющего более 100 тыс. абонентов, класс системы – К1) всегда приводит к значительным негативным последствиям для меня как субъекта, а вот попадание в открытый доступ данных о моих доходах за длительный срок из системы расчета заработной платы (класс системы, как правило, К3), имеет для меня незначительные негативные последствия. Я как субъект с этим категорически не согласен, и считаю, что дело обстоит ровно наоборот. Но возможности повлиять на выбор класса, оценку последствий инцидента и выразить по этому поводу свое мнение закон мне не предоставляет. Между тем принимался он, напомню, исключительно с целью обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну – см. ст. 2 ФЗ-152.

Классификация ИСПДн. Предлагаемая методика классификации ИСПДн плохо согласуется с законом, который не содержит, например, такого понятия, как обезличенные персональные данные (представляется, что это вообще не персональные данные), и не позволяет провести грань между данными, идентифицирующими личность, и данными, позволяющими получить о личности дополнительные сведения.

Да и само определение типовой системы как требующей обеспечения только конфиденциальности персональных данных, а специальной – как системы, где требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий), выглядит очень странно. Статья 19 ФЗ-152 четко определяет, что оператор обязан принимать необ-

ходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий. То есть, если следовать закону, типовых систем не должно быть в принципе.

Есть у предлагаемой методики классификации и другие недостатки. Так, любая система, содержащая сведения о состоянии здоровья субъектов, является одновременно и типовой класса К1, и специальной. Мало того, к защите компьютера частнопрактикующего врача, подключенного к Интернету, и сети огромной больницы, имеющей доступ туда же, строго говоря, предъявляются одни и те же требования.

Наконец, так и нет ответа в документах регуляторов о том, как же все-таки классифицируются специальные системы.

Оценка соответствия. Положение Постановления Правительства РФ от 17.11.2007 № 781 о том, что средства защиты информации должны удовлетворять требованиям, устанавливаемым в соответствии с законодательством Российской Федерации, и о прохождении ими процедуры оценки соответствия является одним из камней преткновения при реализации закона. Законодательство никаких требований к СЗИ не устанавливает, существует лишь система обязательной сертификации для средств защиты информации, составляющей государственную тайну. Да и сама сертификация является одним из возможных способов подтверждения соответствия, в то время как способов оценки соответствия закон о техническом регулировании предусматривает гораздо больше.

К сожалению, постановление не определяет, какие способы оценки соответствия допустимы и как эта оценка выполняется. Используя лишь сертификацию, построить действительно надежную систему безопасности невозможно. К средствам защиты некоторых классов нет утвержденных регуляторами требований, как, например, к средствам антивирусной защиты или обнаружения вторжений. Нет и методов оценки соответствия СЗИ для современных технологий, таких как виртуализация, организация терминального доступа и другие, без которых нельзя построить современную высокопроизводительную вычислительную систему. И снова оказывается оператор перед нелегким выбором – обеспечить нужную вычислительную мощность или выполнить некие формальные требования.

Практически весь мир идет путем установления обязанности оператора обеспечивать конфиденциальность и значительного усиления ответственности за инциденты с персональными данными

Проблемы государственные

Казалось бы, очевидно, что пример выполнения установленных законом и подзаконными актами требований должны показывать органы государственной власти, являющиеся операторами персональных данных. Но никакого другого чувства, кроме недоумения, порталы государственных органов, обрабатывающих сведения о гражданах, у специалистов не вызывают. Для шифрования персональных данных, передаваемых в сети Интернет на портал и с портала государственных услуг www.gosuslugi.ru, применяется протокол https, использующий в свою очередь Open SSL, естественно, никакого сертификата ФСБ не имеющий. А приказ Минэкономразвития вообще запрещает шифровать персональные данные на сайтах госорганов и использовать для доступа к ним дополнительный софт на стороне клиента. На портале ФНС nalog.ru любой человек, знающий ИНН какого-либо гражданина, может получить исчерпывающую информацию о его задолженностях по всем налогам. ИНН никак нельзя считать конфиденциальными сведениями, он доступен из многих источников, поэтому налицо очевидное нарушение права граждан на тайну личной жизни. Аналогичная ситуация и с сайтом службы судебных приставов, охотно делящимся информацией об исполнительных производствах в отношении любого гражданина. ГИБДД и вовсе сообщила о намерении создать общедоступную базу о нарушителях ПДД. Очень хотелось бы знать, нормой какого закона руководствовалась инспекция, намереваясь перевести эти сведения в категорию общедоступных.

Принадлежат все эти сайты неизвестным операторам, отсутствуют предусмотренные законом сведения о целях и способах обработки данных на них, неизвестен класс используемых для этого систем и то, каким способом реализованы на них требования Постановления № 781 в части обеспечения безопасности. Поскольку неизве-

стен оператор, нельзя узнать, направлял ли он уведомление в Роскомнадзор и что в этом уведомлении указано. Если владельцем портала является не орган власти, который обрабатывает персональные данные, предусмотренные законом (а так обстоит дело с порталом gosuslugi.ru, агрегирующим сведения разных ведомств), очень интересно было бы получить подтверждение согласия граждан на передачу владельцам портала своих персональных данных и порядок отзыва такого согласия.

Ситуация крайне неприятная. После появления этих сайтов очень трудно убедить руководителей коммерческих организаций в необходимости тратить значительные средства на построение подсистемы безопасности, соответствующей взглядам законодателей и регуляторов. Они дружно кивают в сторону государственных порталов и задают естественный вопрос о том, зачем им морочат голову требованиями, если сами госорганы их выполнять не собираются.

Подводя итоги

То, что закон о персональных данных будет меняться, было очевидно всем специалистам с момента его принятия. Да и процесс совершенствования законодательства – естественный и неизбежный. Но уж слишком много в ФЗ-152 нестыковок, недоговоренностей и противоречий. С 2005 г. не может перейти в стадию второго чтения проект закона о внесении изменений в законодательные акты, связанные с ратификацией Европейской конвенции и принятием закона о персональных данных. Предполагалось внести изменения в 23 закона, но вот уже пять лет дело не может сдвинуться с мертвой точки. Давно прошел месяц, отведенный в прошлом году Советом Думы на подготовку новых предложений. Значительно выросло и число законов, нуждающихся в корректировке. В случае принятия законопроекта, внесенного В.М. Резником, придется менять все законы, определяющие случаи обязательной обработки персональных данных, поскольку в законопроекте выдвигаются очень жесткие требования к содержанию таких законов.

Решает этот законопроект далеко не все проблемы закона нынешнего, в том числе затронутые в данной статье. Трудно сказать, как будет выглядеть проект после второго чтения, но его принятие может породить и новые проблемы. Так, предлагаемая в законопроекте формулировка: «При обработке персональных данных на основе согласия перечень мер по обеспечению безопасности персональных данных при их обработке определяется соглашением оператора и субъекта персональных данных» приведет, скорее всего, к тому, что в договоре между оператором и субъектом будет указано, что субъект согласен с уровнем защиты персональных данных, предусмотренным оператором. Как она организована, узнать будет невозможно. Учитывая, что законопроект предполагает выдвижение обязательных требований только для государственных и муниципальных систем в случаях, прямо предусмотренных законом, можно будет поставить крест на теме технической защиты в коммерческих организациях и для удовлетворения собственных нужд органов власти (когда обработка идет не на основании нормы конкретного закона). Такая схема обеспечения безопасности обработки сведений о гражданах могла бы заработать только в случае значительного усиления ответственности за инциденты с данными, наносящие ущерб их владельцам. Но таких изменений в законодательстве пока не предполагается.

И еще. В ситуации постоянных изменений правил игры пострадавшими оказываются наиболее законопослушные операторы. Заменили они свои межсетевые экраны на сертифицированные по третьему классу (дорогие и сложные), провели аттестацию своих информационных систем – но больше этого не требуется. Начальнику подразделения информационной безопасности теперь очень трудно объяснить своему руководству, на что были потрачены деньги. И вряд ли средства будут выделены в следующий раз, когда понадобится выполнить, может быть, очень правильные, но совсем не нужные бизнесу требования государственных органов.

Закон и принятые для его реализации акты менять и совершенствовать, безусловно, нужно. Плохо, если это будет происходить, как и раньше, – келейно, без привлечения специалистов-практиков, без учета баланса интересов всех участников процесса и экономической целесообразности затрат на выполнение требований. ИКС

В ситуации постоянных изменений правил игры пострадавшими оказываются наиболее законопослушные операторы

Мне с башни видно всё, или Бизнес – людям

У интересов бизнеса и местных органов власти есть точка пересечения, и лежит она в сфере социальной ответственности. В результате совместных усилий сторон возникает мощный синергический эффект, благодаря которому каждый из партнеров продвигается вперед. Иллюстрация кэтому тезису – Лужский район Ленинградской области.

Запрос администрации

Лужский муниципальный район Ленинградской области знаменит своими лесами и холмами, озерами и реками. В нем находится сразу несколько особо охраняемых природных территорий, в том числе федеральный комплексный заказник «Мшистое болото», шесть заказников регионального значения и несколько геологических памятников природы.

Понимая необходимость сохранения этих богатств, администрация Лужского района еще несколько лет назад назвала улучшение экологического состояния, недопущение утраты потенциала возобновляемых природных ресурсов одним из приоритетных направлений развития муниципального образования.

Между тем нынешнее лето – когда Ленинградскую область хоть и гораздо меньше, чем центральные районы России, затронули лесные пожары, зато дважды посетили ураганы, – показало руководителям района, что традиционных, отработанных способов сохранения природы с привлечением большого числа людских ресурсов уже недостаточно. Нужно брать на вооружение современные технические средства, которые позволили бы предупреждать или моментально реагировать на возникающие в районе чрезвычайные ситуации.

«Мы искали недорогой способ проведения мониторинга пожарной безопасности всей территории района: участков, на которых располагается лес, сельскохозяйственные угодья, наши поселения», – говорит Олег Торжков, первый заместитель главы администрации Лужского муниципального района.

Потребности бизнеса

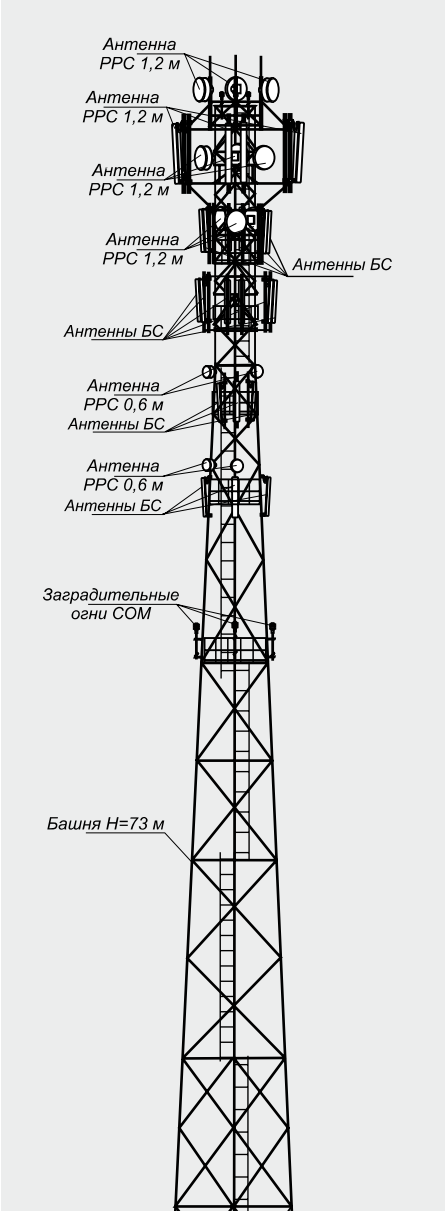
С недавних пор в Ленинградской области начала развертывать сеть антенно-мачтовых сооружений (АМС) для совместного использования операторами сотовой связи независимая компания «Русские Башни». В настоящее время на территории области компания строит сразу 58 высотных объектов, каждый из которых представляет собой полноценный сайт, где одновременно могут разместить свое радиооборудование от трех до пяти операторов сотовой (и не только) связи и где располагается вся необходимая инфраструктура для обеспечения его работы (см. рисунок).

Вокруг всех башенных сооружений установлено ограждение, к ним подведено электропитание в соответствии с Правилами устройства электроустановок (ПУЭ) для потребителей этой категории. На этих объектах размещаются также контейнеры для установки оборудования и датчики системы мониторинга. Последние позволяют отслеживать любое движение вблизи ограждения АМС, возникновение задымления, наличие/отсутствие электропитания и данные о текущем энергопотреблении объекта в режиме реального времени с центрального пульта компании «Русские Башни».

Естественно, такие высотные объекты размещаются на территориях, где компаниям сотовой связи требуется организовать радиопокрытие с нуля или улучшить уже существующее. «Сегодня операторы, – говорит Дмитрий Нелюбов, генеральный директор ЗАО «Русские Башни», – сами указывают такие точки на карте, поскольку в их интересах, чтобы антенно-мачтовые сооружения появлялись там не за их, а за наши деньги». И это неудивительно: возможность арендовать высотные объекты позволит компаниям сотовой связи не отвлекать ресурсы на строительство, а направить их на расширение радиопокрытия сетей, улучшение качества связи, эволюцию к сетям следующих поколений – от UMTS к HPSA и к HSPA+, а в перспективе и к LTE, установка на развитие которой была дана Президентом РФ Д.А. Медведевым. Операторы, как и их зарубежные коллеги, смогут предоставлять абонентам из российской глубинки самые современные услуги на базе беспроводной широкополосной передачи данных, в том числе и стандарта мобильного WiMAX.

Однако окончательный выбор участка для возведения башен возможен только при выполнении двух условий: во-первых, при наличии доброй воли у

Размещение оборудования на башне высотой 73 м



администрации муниципального района, ее готовности найти в указанном месте землю несельскохозяйственного назначения, имеющую границы и владельца, с хорошими подъездными путями и расположенной неподалеку линией электропередач. А во-вторых – при отсутствии возражений у жителей близлежащих населенных пунктов.

Впрочем, для жителей появление в лесу, неподалеку, такой вышки, имеет свои плюсы. Несмотря на то что сотовая связь в России развивается уже более 15 лет, опыт работы «Русских Башен» в Северо-Западном регионе показывает: «медвежьих углов», до которых не добрался пока ни один оператор, в глубинке еще хватает.

Интересы администрации Лужского района, озабоченной поиском средства мониторинга пожарной безопасности лесных угодий для защиты от огня, и компании «Русские Башни», которой важно было получить участки в лесах для строительства вышек, просто не могли в некоторой точке не пересечься. Это пересечение интересов местной власти и бизнеса и обеспечило…

Еще немного – и в работу

Синергический эффект

В результате столь удачной синергии обе стороны не просто смогли решить стоящие перед ними задачи, но и нашли для этого наиболее эффективный с экономической точки зрения способ. Администрация Лужского муниципального района Ленинградской области и ЗАО «Русские Башни» подписали соглашение о размещении на высотных объектах, принадлежащих компании, IP-видеокамер для наблюдения за пожарной безопасностью прилегающих лесных массивов.

С технической точки зрения в построении системы видеонаблюдения с использованием веб-камер, изображение с которых передается по IP-протоколу на пульт диспетчера, нет ничего принципиально нового. Такое решение давно и широко используется при организации охраны объектов недвижимости в городах и дачных поселках. Однако нынешнее лето показало, что видеонаблюдение очень востребовано и в лесу. И, пожалуй, впервые для его реализации было решено задействовать башни, совместно используемые операторами сотовой связи.

Решение для мониторинга на основе IP-телекамер, установленных на башнях на отдаленных участках и работающих по заданному алгоритму, и по стоимости, и по охвату территории несравнимо эффективнее того, что обеспечивают беспилотные летательные аппараты. Для видеонаблюдения не требуется присутствие человека, оно ведется круглые сутки в любую погоду. Своевременно поданный сигнал о возгорании в лесном массиве окажет неоценимую помощь лесным хозяйствам, тем более учитывая хроническую нехватку кадров у них. А главное, это решение не требует больших затрат от местной администрации.

По соглашению между администрацией Лужского муниципального района и ЗАО «Русские Башни» на первом этапе проекта IP-камеры будут установлены на четырех строящихся сейчас в районе башенных сооружениях – в Луге, Волошево, Тесово 4 и в Покровке. Видеоинформация с них, а также показания установленных на высотных объектах датчиков через Интернет или в виде MMS будут передаваться на пульт районной службы спасения, а также лично главе администрации Лужского района В.П. Ейбогину для оперативного реагирования на чрезвычайные ситуации.

Добавим, что совместный проект с компанией «Русские Башни» дает администрации Лужского района возможность попутно решить еще одну стратегическую задачу, обозначенную в Концепции развития района с 2008 по 2017 гг., – обеспечить полное покрытие его территории телефонной связью, в том числе мобильной.

О своей инициативе по созданию собственной системы видеонаблюдения администрация Лужского района пока широко не объявляла, тем не менее в ее планах на будущее – опробовать это решение, научиться извлекать пользу из всех его возможностей и передать этот опыт другим районам. По словам Дмитрия Нелюбова, интерес местной администрации к развитию проекта настолько велик, что после сдачи первых АМС в эксплуатацию вполне возможно появление в районе от трех до пяти дополнительных высотных объектов ЗАО «Русские Башни». Это и неудивительно: учитывая наличие всех необходимых коммуникаций, включая каналы связи, IP-видеокамеры на башнях можно использовать для решения самых разных задач: от предупреждения жителей о надвигающихся атмосферных фронтах и ураганах до его защиты от возможных терактов. Например, автоматика, установленная на каждой башне, очень помогла бы при ликвидации последствий недавнего урагана в Ленобласти, который обесточил более 1200 населенных пунктов. Благодаря ей можно было бы практически сразу определить границы зоны бедствия, скоординировать действия энергетиков, коммунальных служб, МЧС.

К слову, в ближайших планах компании «Русские Башни» – заключение партнерских соглашений с Гидрометцентром о мониторинге погоды. О таком количестве автоматических станций совсем недавно метеорологи не могли и мечтать! У них появится возможность оперативно получать данные с башен, разбросанных по огромной территории, а значит, более точно строить долгосрочные прогнозы.

Александра КРЫЛОВА

РУССКИЕ БАШНИ
www.rtowers.ru

Регулирование 2.0
С точки зрения мира

«Без четкой и ясной стратегии нельзя жить дальше и строить информационное общество с электронным государством».
Н.С. Мардер
(Из выступления на конференции NGN'2009)

Говорят, что бюрократия, выбирая между «рано» и «поздно», всегда голосует за «поздно», лелея надежду превратить его в «никогда». Однако инициаторами многих начинаний являются как раз отраслевые бюрократы. А это значит, что движение вперед выгодно всем. И это внушает...

Александр ГОЛЫШКО,
канд. техн. наук

Даешь ШПД!

По сообщениям Cellular News, в МСЭ сформирована группа во главе с мексиканским миллиардером Карлосом Слимом и президентом Руанды Полем Кагаме с целью развития широкополосного доступа в странах с низким проникновением Интернета. В группу вошли руководители 30 ведущих телеком-компаний, представители ООН, бизнесмены и общественные деятели. Основной задачей группы станет разработка стратегии достижения глобального охвата широкополосных сетей и их использования для медицинского обслуживания, образования и охраны окружающей среды.

ЕС нуждается в усилении регуляторной функции

По данным CyberSecurity, современное развитие телекоммуникационных технологий в Европе уступает показателям как США, так и Японии и Южной Кореи. Поэтому в Еврокомиссии подготовлен внутренний доклад, в котором утверждается, что ЕС необходимо иметь мощные рычаги влияния на национальных регуляторов отрасли с целью создания единого цифрового пространства. В частности, под контроль ЕС должны отойти: недавно начавшийся процесс освоения цифрового дивиденда, панъевропейская электронная торговля, защита прав потребителей, лицензирование контента и др.

Сегодня в Европе насчитывается слишком много «цифровых девственников», тогда как Еврокомиссия собиралась уже к 2013 г. обеспечить всех граждан ЕС широкополосным доступом в Сеть. Пока лишь 25% европейцев используют ШПД, 30% вообще никогда не пользовались Интернетом и лишь 1% европейцев выходят в Сеть через перспективные волоконно-оптические каналы. В Японии же этот показатель составляет 12%, в Южной Корее – 15%.

Поддержка голосовых услуг неэффективна

Федеральная комиссия по связи США (FCC) сделала первый шаг к превращению фонда Universal Service Fund из инструмента поддержки сетей, предоставляющих традиционные услуги телефонии, в эффективный и действенный инструмент создания высококачественных широкополосных услуг, доступных всем американцам. В национальном плане по широкополосной связи, направленном комиссией в Конгресс весной 2010 г., указано на необходимость всеобъемлющей реформы универсальных услуг, которая не стала бы дополнительным бременем для потребителей.

Законодательство по универсальным услугам устарело

По сообщениям Dow Jones Newswires, Еврокомиссия планирует изменить законодательство от 2002 г. об универсальных услугах (базовые телефонные услуги и интернет-услуги для наиболее удаленных регионов Европы). Комиссия обеспокоена тем, что эти правила устарели и должны быть распространены на ШПД, и начинает мониторинг «отраслевого мнения» на этот счет.

Зачем AT&T нужен Skype?

Как сообщает Light Reading Mobile, компания Skype объявила, что владельцы iPhone могут совершать вызовы «Skype–Skype» «поверх» 3G-сети AT&T. Обновленный сервис Skype 2.0 будет предоставляться на безвозмездной основе до

2011 г. В чем же выгода оператора от реализации услуги Skype?

По словам Дарио Талмесио, аналитика Informa Telecoms & Media, AT&T, с одной стороны, создает условия для каннибализации доходов мобильных операторов путем замещения традиционных голосовых услуг сервисами VoIP, т.е. именно того, чего операторы давно опасались. С другой стороны, стратегия AT&T, очевидно, состоит в обеспечении собственного участия в цепочке добавленной стоимости VoIP и стремлении восполнить неизбежную потерю доходов от традиционного голоса за счет услуг передачи данных. Кроме того, партнерство со Skype позволит компании привлечь новых клиентов. Как показал опыт Великобритании, многие абоненты готовы сменить оператора только из-за возможности использования мобильного сервиса Skype.

Согласно исследованию Juniper Research, услуга мобильного VoIP будет привлекать абонентов 3G и Wi-Fi до 2012 г., когда 100 млн абонентов 3G будут одновременно и абонентами VoIP. При этом высокий спрос на мобильный VoIP будет стимулировать развитие именно сетей Wi-Fi, а не 3G, в результате чего операторы мобильной связи к 2015 г. потеряют до $ 5 млрд. Очевидно, что в таких условиях необходимым элементом стратегии операторов должно стать получение доли в цепочке добавленной стоимости мобильного VoIP.

Мобильный ШПД самодостаточен

Компания Nokia Siemens Networks опубликовала технико-экономическое исследование, доказывающее, что услуги мобильного широкополосного доступа в Интернет являются самодостаточным бизнесом. Операторы могут выгодно предоставлять услуги передачи данных в объеме до 5 Гбайт в месяц на абонента с использованием технологий HSPA и LTE в нескольких частотных диапазонах на существующей инфраструктуре сети. При этом чем выше уровень проникновения мобильного ШПД, тем меньше стоимость доставки гигабайта данных на одного абонента.

Исследование показало, что можно добиться и экономии капитальных и операционных затрат. Например, при условии обслуживания на сайте базовой станции 500 абонентов, каждый из которых потребляет 2 Гбайт в месяц, показатели CAPEX и OPEX будут менее 3 евро на абонента в месяц. При дальнейшем повышении плотности абонентов можно уменьшить ежемесячные CAPEX и OPEX до уровня 2 евро и ниже.

Ответный удар «мобильной империи»

По информации Light Reading Mobile, консорциум из крупнейших операторов сотовой связи планирует создать промышленный стандарт разработки приложений для мобильных устройств, базирующийся на веб-технологии мобильных виджетов. Так операторы отреагировали на неуклонное ослабление их позиций на рынке мобильных приложений по сравнению с проектами «гуглоподобных» поставщиков сервиса.

Проблема рынка мобильных приложений сегодня, как видят ее операторы, заключается в вертикальной структуре существующих бизнес-моделей, применяемых компаниями Apple, Google, Nokia и Research In Motion.

Консорциум Wholesale Applications Community (WAC), созданный в феврале 2010 г., ставит своей целью устранить фрагментацию на рынке мобильных приложений, а именно упростить процесс разработки и обеспечить кросс-функциональность приложений для различных устройств, операционных систем и сетей. Члены альянса также надеются установить руководящие принципы для новой бизнес-модели, добиваясь последовательного распределения доходов по всей цепочке добавленной стоимости – от разработчика приложений и оператора связи до владельца магазина.

К настоящему моменту группа WAC выросла до 29 членов, включая AT&T, Deutsche Telekom, NTT DoCoMo, Orange, Softbank, Telefonica, Vodafone и др. Члены консорциума надеются, что использование технологий, не зависящих от устройств и сетей, позволит стимулировать развитие рынка и сделать широкий круг мобильных приложений доступным миллиардам абонентов по всему миру.

Зачем нужен «цифровой дивиденд»

Как пишет Cellular News, Еврокомиссия решительно поддерживает использование частот 790–862 МГц, в настоящее время задействованных для эфирного вещания в большинстве государств-членов ЕС, для развертывания широкополосных интернет-услуг в сетях LTE и WiMAX. Руководство комиссии рассчитывает, что этот шаг до 2013 г. принесет экономике ЕС 44 млрд евро и поможет достичь стратегических целей развития Евросоюза до 2020 г. Эксперты отрасли полагают, что сетевая инфраструктура для предоставления услуг мобильного ШПД в диапазоне 800 МГц будет до 70% дешевле используемой в настоящее время в сетях 3G. Данный факт, безусловно, сделает инвестиции в развитие сетей более привлекательными, что в конечном счете положительно скажется на качестве и доступности широкополосных интернет-услуг.

FCC продолжает освобождать частоты для беспроводного ШПД

По сообщениям FierceWireless, FCC, придавая большое значение развитию услуг мобильного ШПД в стране, объявила о стратегии высвобождения частот в объеме 500 МГц в течение следующих 10 лет, причем из них 300 МГц – в ближайшие пять.

В рамках этой инициативы FCC недавно выпустила официальный запрос о возможности задействования диапазона шириной 35 МГц, так называемого Big LEO, для беспроводных широкополосных сетей. Сегодня этот диапазон, 1675–1710 МГц, используется метеозондами и спутниками.

FCC уже одобрила план высвобождения 25 МГц в диапазоне 2,3 ГГц и собирается к 2015 г. «оторвать» еще 120 МГц от эфирного ТВ-вещания. Для этого она планирует провести аудит текущего использования спектра и перераспределить его в пользу более эффективных сегментов отрасли. FCC также хочет, чтобы ряд телекомпаний рассмотрели возможность совместного

использования спектра и передачи нескольких потоков HD там, где раньше был один канал. Все высвобожденные частоты будут проданы на аукционе в индустрии мобильной связи.

«Оптическая» Австралия

Как сообщает Ars Technica, власти Австралии заручились поддержкой крупнейшего провайдера страны Telstra в проекте перехода на оптоволоконные каналы связи. Telstra откажется от всех остальных проводных каналов связи, заменив их оптоволокном. Эта договоренность – часть правительственной инициативы по созданию национальной оптоволоконной сети. На данный проект выделено 43 млрд австралийских долларов ($37,7 млрд). Перевод всех абонентов на оптоволокно обойдется Telstra в 9 млрд австралийских долларов ($7,9 млрд). В программу входит не только прокладка «оптики»: удаленные сельскохозяйственные районы смогут подключиться к Сети по беспроводным каналам связи.

Операторы могут выгодно предоставлять услуги мобильного ШПД в объеме до 5 Гбайт в месяц на абонента с использованием технологий HSPA и LTE на существующей инфраструктуре сети

«Оптическая» Германия

Deutsche Telekom объявила о новой стратегии, которая сконцентрирована на мобильных данных, высокоскоростной широкополосной связи и ИТ-услугах, и которая, как надеется компания, превратит ее из оператора в «оператора плюс», позволив к 2015 г. удвоить доходы в пяти конкретных областях: мобильном Интернете, double и triple play, онлайн-услугах (включая магазины приложений и веб-хостинг), ИТ-услугах (в том числе облачных сервисах подразделения T-Systems International), а также Intelligent Network Solutions (в таких вертикалях, как энергетика, здравоохранение, средства массовой информации и транспорт). Эти направления бизнеса в 2009 г. принесли компании 15,8 млрд евро, но к 2015 г. DT планирует увеличить эту сумму до 29 млрд евро. Действительно, DT заявляет, что в течение ближайших трех лет вложит более 10 млрд евро в три области – новую оптоволоконную сеть доступа, модернизацию мобильной инфраструктуры, а также совершенствование процессов Service Provider Information Technology (SPIT).

Удешевление роуминга – в законе

Как пишет Light Reading Mobile, Европейский суд высшей инстанции официально поддержал позицию ЕС по внедрению закона, обязывающего мобильных операторов снизить стоимость роуминговых голосовых вызовов для своих абонентов. Четыре крупнейших европейских мобильных оператора – Vodafone Group, O2, T-Mobile и Orange, оспорили в суде законность решения, принятого Евросоюзом в 2007 г. Тогда чиновники обязали операторов значительно снизить расценки на переговоры для абонентов, находящихся в европейском роуминге. В решении суда говорится, что положение о роуминге полностью соответствует закону и «общество имеет право наложить ограничения на предельные тарифы мобильной связи».

Теперь верхний предел стоимости минуты роуминговых звонков для европейских пользователей, находящихся в европейском роуминге, составляет 49 центов для исходящих звонков и 24 цента для входящих, а с 2011 г. цены будут снижены до 35 и 11 центов соответственно. До момента вступления этого закона в силу стоимость минуты роуминга была существенно выше. К примеру, немцы, приезжающие в соседнюю Австрию, были вынуждены платить 1,7 евро за минуту разговора, а бельгийцы, оказавшиеся на Кипре, – 2,5 евро за минуту. Помимо снижения цен на голосовое общение, законом предусмотрено удешевление мобильного интернет-доступа и SMS.

Регуляторы настаивают на предсказуемом счете

По сообщениям AP, в связи с участившимися жалобами абонентов FCC рассматривает законопроект, в рамках которого мобильные операторы будут обязаны заблаговременно информировать своих абонентов об исчерпании средств на счете или их приближении к лимиту в соответствии с тарифным планом при нахождении в роуминге. Аналогичные правила уже действуют в ЕС, требуя от операторов отправки текстового сообщения абонентам, чей баланс счета близок к порогу отключения.

Скорый конец «безлимитки»

По словам руководителя Verizon Wireless Лоуэлла Макадама, подошло время глобального пересмотра операторских тарифов на передачу данных в будущих LTE-сетях, запуск которых уже не за горами. Вместо подписки на передачу данных на каком-либо устройстве куда интереснее выглядит покупка трафика и распределение его на многих гаджетах так, как этого пожелает пользователь. Подоб-

ная схема позволит снизить высокий спрос на безлимитный мобильный ШПД. К примеру, мобильные LTE-коммуникации принесут пользователям 12-мегабитные скорости, HD-видео в реальном времени, многопользовательские игры и круглосуточную подключенность устройств к Сети. А операторам?

Сетевая нейтральность ведет к потере рабочих мест

Цитируя исследование, проведенное экономистом компании The Brattle Group Колеманом Бэйзелоном, Network World пишет, что правила нейтральности сетей, одобренные FCC, в течение следующих 10 лет могут привести к потере 340 тыс. рабочих мест в сфере телекоммуникаций, а расходы широкополосного телеком-сектора в 2011 г. могут снизиться на $5 млрд. По мнению Бэйзелона, FCC должна быть осторожной в развитии любых правил сетевого нейтралитета, чтобы не перечеркнуть собственные цели продвижения широкополосных сетей. Он считает, что распространение ШПД в США и так идет успешно: приблизительно 95% жителей страны доступно подключение к фиксированному ШПД и 98% могут использовать 3G-сервисы. Вместе с тем, защитники нейтральности сетей (среди которых компания AT&T) считают, что утверждения Бэйзелона не подтверждены фактами, а сокращения рабочих мест, как это ни прискорбно, являются для операторов связи общепринятой практикой.

Поставщикам предложат «разоружиться перед партией»

Как сообщила The Economic Times of India, отныне все производители оборудования связи, работающие в Индии, должны будут предоставлять в контролируемый правительством банк данных информацию по исходным кодам и детальному дизайну продуктов и услуг, реализуемых в стране. Это следует из проекта законодательных инициатив, касающихся обеспечения национальной безопасности (а заодно и защиты отечественного производителя). Особенность новых законопроектов в том, что мобильные операторы могут делиться информацией из базы с поставщиками, которые обслуживают их сети.

Правительство США введет удостоверения личности в Интернете

Как пишет Ruformator, департамент кибербезопасности Белого дома опубликовал «Национальную стратегию доверительной идентификации в киберпространстве». Основная цель – сделать онлайн-транзакции более безопасными. В документе описывается еще не разработанная система, с помощью которой каждый пользователь сможет на добровольной основе получить у одного из провайдеров индивидуальный идентификатор. Этот сертификат будет использоваться при покупках и переводе средств для подтверждения личности покупателя. Его предполагается задействовать не только в платежных системах, но и в качестве универсального ключа для всех веб-сервисов, включая социальные сети и электронную почту.

А по сообщениям CNET News, в Сенат США внесен законопроект, предлагающий предоставить президенту страны широкие полномочия по управлению Интернетом в случае чрезвычайного положения. В связи с этим при Министерстве национальной безопасности США предложено создать Национальный центр сетевой безопасности и коммуникаций. В случае объявления в стране чрезвычайного положения Центру должны подчиняться все американские компании, деятельность которых связана с предоставлением услуг связи или ИТ-услуг, т.е. интернет-провайдеры, поисковые системы и производители ПО.

Интернет как одно из прав человека

По результатам опроса, проведенного BBC World Service, около 87% пользователей Интернета считают, что доступ в Сеть должен стать одним из основных прав человека.

По сообщениям Paul Budde Communication, в течение последних двух лет правительства ряда стран признали, что полноценная национальная широкополосная инфраструктура имеет важнейшее значение для социального развития, экономического роста и потенциала страны, а также позволяет сохранить и привлечь квалифицированные рабочие кадры.

В Швейцарии с 2008 г. в понятие универсальной услуги связи включен ШПД в Интернет по регулируемой цене. В Финляндии ШПД станет частью универсальной услуги с декабря 2010 г., в Испании – с 2011 г. Франция, Великобритания и Италия примут аналогичные законы в 2012 г. Ожидается, что к 2013 г. ШПД станет обязательным для всех стран ЕС, при этом требуемая минимальная пропускная способность канала к 2020 г. составит не менее 30 Мбит/с.

Правительствами разрабатываются схемы финансирования создания широкополосной инфраструктуры. Так, во Франции с 2008 г. обязательна установка оптоволокна, разделяемого всеми операторами, в существующие и строящиеся здания. В результате Париж сейчас – единственный город в мире с четырьмя конкурирующими операторами, использующими технологии FTTx. Подобная картина и в Швейцарии, где совместный доступ к последней миле реализуется посредством разделения операторами общей стоимости ее развертывания.

В Финляндии согласно «широкополосному плану», состоящему в обеспечении оптоволоконного широкополосного доступа для всех граждан к 2015 г., правительство будет покрывать треть стоимости строительства в районах с низким коммерческим потенциалом. Оставшаяся часть будет обеспечиваться операторами, муниципалитетами и финансовой поддержкой со стороны Евросоюза. Затраты правительства будут компенсироваться платежами, взимаемыми с телекоммуникационных компаний.

■ ■ ■

О том, как ростки зарубежного регулирования можно привить к российскому нормативно-правовому древу, мы поговорим в следующий раз. ИКС

Управляемый климат

Выделение тепла – неотъемлемое свойство любого электрического и электронного оборудования. При размещении такого оборудования в закрытых шкафах, стойках, корпусах неизменно возникает вопрос: как поддерживать необходимую температуру внутри шкафа либо стойки? Ответ на него дают системы контроля микроклимата Rittal, отличительные черты которых – качество, инновации, энергоэффективность.

Игорь ЗАНЕГИН,
ведущий специалист
Академии Rittal

Компания Rittal GmbH & Co, KG (Германия), известная как ведущий мировой производитель корпусного и шкафного оборудования для промышленности и ИТ, вот уже 25 лет занимается вопросами эффективного охлаждения корпусов. Компания располагает собственным производством климатического оборудования, научно-исследовательской базой, а также всемирной службой сервиса для компонентов контроля микроклимата. Это позволяет предложить заказчику самый широкий спектр продуктов и решений – от вентиляции корпусов до высокомощного жидкостного охлаждения.

Поскольку проблема отвода тепла из корпусов в одинаковой степени актуальна как для промышленного, так и для ИТ-оборудования, Rittal выпускает решения для обеих этих областей.

Шадящие условия: вентиляция корпусов

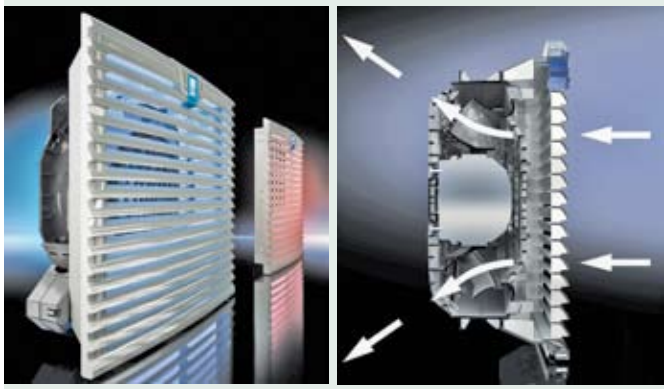
Если тепловыделение оборудования внутри корпуса не превышает нескольких киловатт, а температура в помещении, где установлено оборудование, всегда ниже, чем должна быть внутри корпуса, наилучшее решение для охлаждения – вентиляция корпуса окружающим воздухом. В зависимости от вида оборудования и запыленности помещения Rittal предлагает разнообразные решения для вентиляции корпусов.

Для шкафов с телекоммуникационным оборудованием и оборудованием кабельных сетей обычно применяют потолочные вентиляторы (одиночные или панели из нескольких вентиляторов), которые обеспечивают ток воздуха внутри корпуса в направлении снизу вверх. Для охлаждения 19" серверов предлагаются стойки с перфорированными дверями, а также специальные траверсы с вентиляторами, монтируемые на задние двери таких стоек.

В условиях промышленного производства в воздухе часто содержится много пыли и грязи. Поэтому для корпусов с оборудованием, помимо вентиляции, актуален вопрос о сохранении высокой степени защиты (IP) от попадания вовнутрь пыли и воды. Наилучшим решением здесь являются фильтрующие вентиляторы, которые монтируются в вырезы в вертикальной поверхности корпуса. Помимо собственно вентилятора, который может работать как на вдув, так и на выдув воздуха из шкафа, устанавливается выходной (входной) фильтр – решетка, за счет которой создается направленный поток воздуха через корпус. Вентилятор и выходной фильтр оснащены фильтрующими прокладками, благодаря которым корпус имеет степень защиты IP 54. Если заменить стандартные прокладки прокладками тонкой очистки, а также оснастить вентиляторы и фильтры специальным защитным кожухом, то можно обеспечить и более высокую степень защиты – до IP 56.

Весной 2010 г. компания Rittal представила новую серию фильтрующих вентиляторов TopTherm (рис. 1), в которой впервые в мире в качестве фильтрующих были использованы так называемые диагональные вентиляторы. Преимуществом диагональных вентиляторов перед традиционными осевыми является то, что воздух от такого вентилятора вдувается в корпус не направленным потоком, а в виде конуса, под углом к оси вентилятора. Это способствует максимально равномерному распределению охлаждающего воздуха внутри корпуса и предотвращает появление "горячих точек". Кроме того, фильтрующая прокладка диагонального вентилятора при наличии пыли в воздухе загрязняется равномернее, что делает давление воздуха более стабильным и позволяет реже проводить замену и чистку прокладок. Наконец, все стандартные операции с вентиляторами новой серии – монтаж на шкаф, смена направления потока и места подключения питания – выполняются без помощи инструментов.

Рис. 1. Диагональный фильтрующий вентилятор TopTherm



Средний класс – холодильные агрегаты для шкафов и корпусов

Если температура внутри корпуса должна быть ниже температуры окружающей среды или равна ей, то пря-

Рис. 2. Настенные и потолочные холодильные агрегаты, двери для контроля микроклимата

мая вентиляция корпуса становится невозможной, и для него необходим собственный источник холода. Одним из источников может служить холодильный агрегат – главный продукт Rittal в семействе систем контроля микроклимата. Rittal предлагает три основных типа таких агрегатов – потолочные, настенные агрегаты и двери для шкафов TS 8 с интегрируемым модулем охлаждения (рис. 2). Все эти агрегаты представляют собой автономную компрессорную холодильную установку с двумя независимыми воздушными контурами (внешний и внутренний воздух) и контуром охлаждения с экологически чистым хладагентом R134a. Номинальная мощность охлаждения агрегатов составляет от 300 Вт до 4 кВт. Для настенных агрегатов мощностью 1 и 2 кВт, помимо стандартного исполнения, Rittal предлагает энергосберегающую серию Cool Efficiency. Энергопотребление таких агрегатов на величину до 45% меньше, чем у аналогичных стандартных агрегатов.

Агрегат управляется встроенным микроконтроллером, который в отдельных случаях можно интегрировать во внешние системы управления и автоматики. Все агрегаты номинальной мощностью от 1 кВт имеют встроенный испаритель конденсата. Чтобы предотвратить отложение пыли, конденсаторы всех агрегатов покрывают грязеотталкивающим покрытием RiNano, благодаря чему значительно упрощаются работы по обслуживанию агрегатов.

Экстремальные условия – жидкостное охлаждение

В последние годы задача отвода больших количеств тепла от стоек и корпусов приобрела особую актуальность. Это связано прежде всего с миниатюризацией электронных компонентов и увеличением плотности оборудования внутри корпуса, что, в свою очередь, приводит к значительному росту тепловыделения. Поскольку теплоемкость воды примерно в 4000 раз выше теплоемкости воздуха, жидкостное охлаждение корпусов обеспечивает более широкие возможности по сравнению с традиционным воздушным охлаждением. Кроме того, нередки случаи, когда высокая температура окружающей среды делает невозможной не только вентиляцию шкафа, но и эксплуатацию холодильного агрегата.

Для охлаждения серверных стоек с высоким тепловыделением на стойку (до 30 кВт) Rittal предлагает семейство воздухо-водяных теплообменников Liquid Cooling Package (LCP). Такой теплообменник пристыковывается к специальной герметичной серверной стойке и позволяет – в зависимости от модели и конфигурации – отвести от стойки до 30 кВт тепловыделения. Это решение особенно актуально для стоек, в которых размещаются блейд-серверы.

Из промышленного оборудования традиционно высоким тепловыделением характеризуются преобразователи частоты вращения. Для таких устройств в программе продуктов Rittal имеются специальные водоохлаждаемые монтажные панели Direct Cooling Package (DCP). Несмотря на небольшие размеры (ширина до 1000 мм, высота до 400 мм), с помощью такой монтажной панели можно отвести до 6 кВт тепла непосредственно от того места в корпусе, где это тепло физически возникает.

Наконец, воздухо-водяные теплообменники незаменимы для корпусов в условиях сильной запыленности и наличия в воздухе едких и агрессивных веществ, что также затрудняет применение систем воздушного охлаждения.

Главным преимуществом всех систем жидкостного охлаждения является то, что мощность охлаждения не зависит от температуры окружающей среды в помещении, где установлен корпус. Это не только значительно снижает затраты на кондиционирование помещений, но и позволяет добиться максимальной компактности технического решения.

Единственное необходимое условие для применения жидкостного охлаждения – наличие внешней водоохлаждающей установки (чиллера), который подготавливает охлаждающую воду нужной температуры и подает ее на объект охлаждения (теплообменник или панель DCP).

Таким образом, в портфеле компании Rittal имеется полный спектр решений для охлаждения корпусов и высокопроизводительного оборудования. Помимо собственно продуктов, компания всегда готова предложить полную поддержку в области проектирования, расчета и подбора систем контроля микроклимата, а также специализированное программное обеспечение для подбора систем контроля микроклимата Rittal Therm. Целью компании является не только решение технических проблем заказчиков, но и обеспечение максимальной энергоэффективности этих решений.

ООО «Риттал»
123007, Россия, г. Москва,
ул. 4-я Магистральная, д. 11, стр. 1
Тел.: (495) 775-0230, факс: (495) 775-0239
info@rittal.ru, www.rittal.ru

Цифровое мобильное телевидение готовится выйти в массы

В России тестируется одна из первых сетей мобильного ТВ, основанная на стандарте DVB-H.

Дмитрий СЕМЕНОВ, руководитель службы планирования и строительства сети ООО «Доминанта»

Левон ДАДАЯН, руководитель службы эксплуатации ООО «Доминанта», канд. техн. наук

Тестирование с декабря 2009 г. проводит один из пионеров в развитии мобильного телевидения* в России – компания «Доминанта», входящая в ГК «ВымпелКом» (структуру сети см. на рис. 1). Вещание в Москве осуществляется на 26-м телевизионном канале (частота 514 МГц).

Структура сети

Головная станция

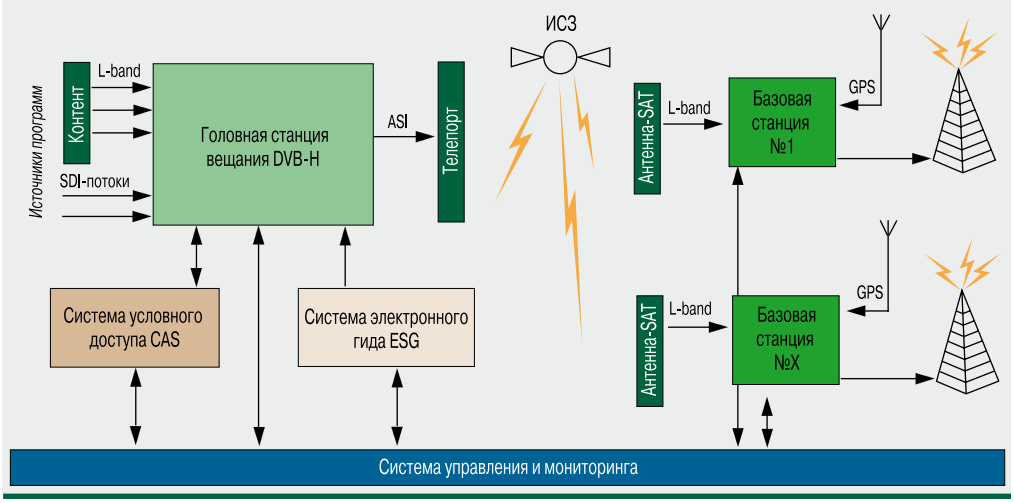
Оборудование формирования сигнала – центральная головная станция (ГС) цифрового телевизионного вещания стандарта DVB-H по способу формирования контента сходна с головными станциями кабельного ТВ и цифрового эфирного ТВ формата DVB-T. Основной контент принимается с помощью профессиональных спутниковых ресиверов. Для доставки контента можно организовать каналы на основе различных протоколов передачи и волоконно-оптических линий, напрямую связанных со студиями телеканалов или центрами формирования медиапотоков. Можно использовать и playout-серверы. Одно из основных условий состоит в том, что на вход головной станции должен подаваться видеосигнал в формате SD-SDI (рис. 2).

Полученный сигнал SDI через матрицу коммутации передается на кодеры, на которых формируется MPEG4-видеопоток форматов VGA (640 × 480), CIF (352 × 288)

Стандарт DVB-H

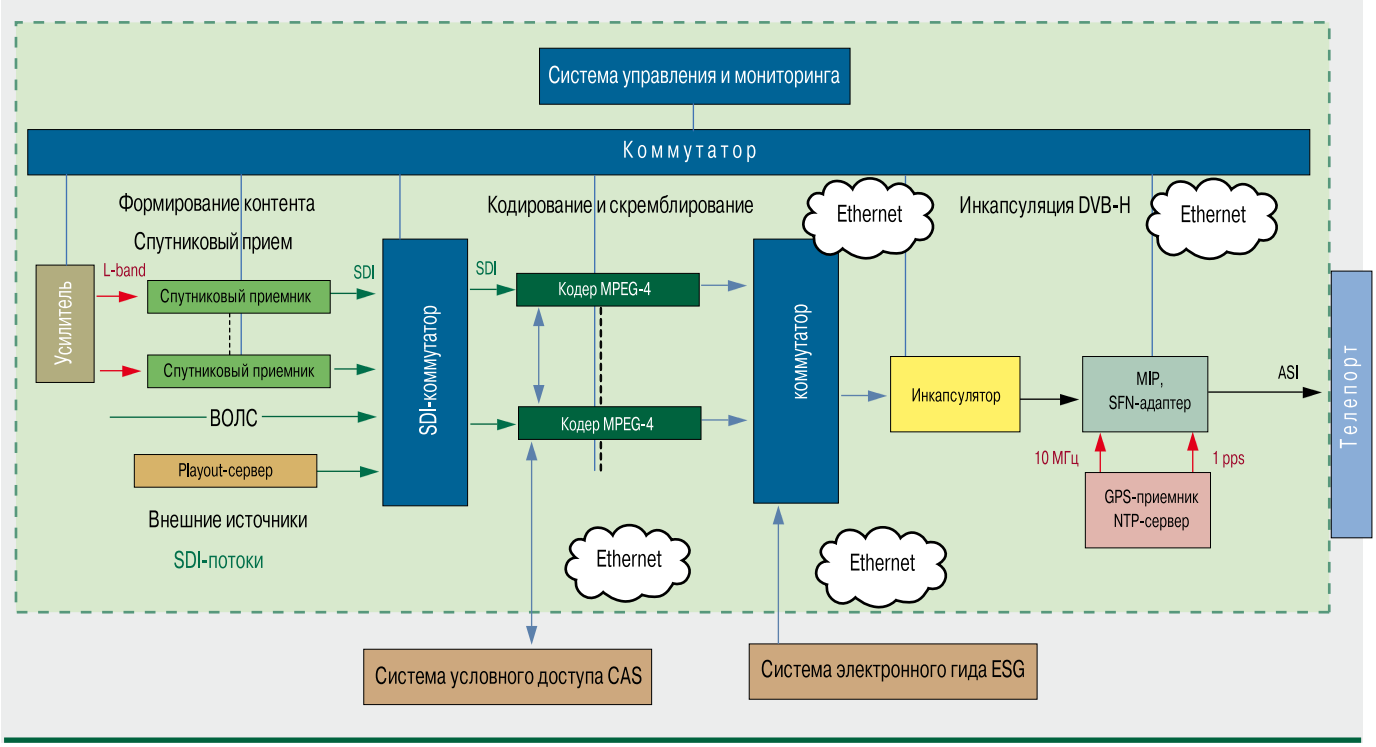
Европейский стандарт DVB-H (Digital Video Broadcasting – Handheld; ETSI EN 302 304, DVB-H – Transmission System for Handheld Terminals) является логическим продолжением стандарта DVB-T (Digital Video Broadcasting – Terrestrial). В нем поддерживаются дополнительные функции, учитывающие требования переносных мобильных устройств с автономным питанием. Для уменьшения расхода питания батарей переносных устройств используется технология квантования сигнала по времени time slicing: принимающее устройство включается только в те интервалы времени, когда передаются наборы данных, соответствующие каналу, на который настроено принимающее устройство. В течение этого короткого времени данные, передающиеся с высокой скоростью, помещаются в буфер принимающего устройства, который может содержать как загруженные данные, так и проигрываемое потоковое видео. Экономия заряда батареи принимающего устройства зависит от соотношения времени его работы на прием и времени ожидания. При трансляции десяти и более сервисов степень экономии электроэнергии принимающим устройством достигает 90%.

Рис. 1. Структурная схема сети DVB-H



* Тестовое вещание в Москве в формате DVB-H с ноября 2009 г. на 36-м канале ведет Yota TB (ООО «Кентавр»). – *Прим. ред.*

Рис. 2. Устройство головной станции



или QVGA (320 × 240). Там же происходит сжатие видеоизображения в стандарте H.264 и закрытие каналов системой условного доступа. Вся связка кодеров работает в режиме статистического кодирования сигналов. Скорость IP-потока на выходе кодера изменяется в широких пределах в зависимости от тематики исходного телеканала и может устанавливаться индивидуально в пределах 100–600 Кбит/с. Например, для телеканала спортивной направленности, транслирующего футбольные или хоккейные матчи, требуется более высокая средняя скорость по сравнению с детским каналом, в программе которого присутствуют в основном мультфильмы и статические изображения. Сформированные потоки с кодированными и закрытыми системой условного доступа CAS телеканалами, а также дополнительные сервисы, такие как система электронного гида ESG, поступают на IP-инкапсулятор, где происходит «упаковка» этих каналов и сервисов в транспортный поток формата MPEG2-TS. На данный момент «Доминанта» распространяет через свою сеть 12 телевизионных каналов.

Системы ESG и CAS

Система электронного гида (Electronic Service Guide, ESG) – это программно-аппаратный комплекс, ответственный за экранное меню, отображающее расписание теле- или радиопрограмм с возможностью интерактивной навигации в контенте по времени, названию канала, жанру и т. д. (см. рекомендации ETSI TS 102, 471 v1.2.1 IP Datacast over DVB-H: Electronic Service Guide (ESG).

Система условного доступа CAS – это программно-аппаратный комплекс, ограничивающий доступ к цифровым телепрограммам. Скремблирование позволяет эффективно реализовать принцип оплаты за просмотр программ.

Через интерфейс ASI транспортный поток MPEG2-TS передается на MIP Inserter, где в этот поток добавляются временные MIP-метки (метки синхронизации, необходимые для работы SFN-сети, когда все передатчики работают на одной частоте), а также информация для передающих устройств базовых станций. Скорость выходного потока имеет фиксированные значения, зависящие от выбранного типа модуляции, относительной скорости кода и величины защитного интервала. При выбранной комбинации параметров сети она составляет 7,37 Мбит/с (тип модуляции QPSK, защитный интервал 1/8, скорость кодирования 2/3). При таких значениях параметров транспортный поток может нести до 16 телевизионных каналов с хорошим качеством при разрешении QVGA и 25 кадрах в секунду.

Система доставки сигнала TS ASI

Доставка сигнала до базовых станций происходит следующим образом: сигнал в формате MPEG2-TS преобразуется в спутниковом модуляторе в поток стандарта DVB-S/S2. Далее средствами наземной передающей станции космической связи поток передается на борт орбитального спутникового ретранслятора. Со спутника идет распространение сигнала на базовые станции. Хочется отметить, что использование более современного стандарта вещания DVB-S2 существенно уменьшает требуемую полосу частот на борту спутникового ретранслятора по сравнению со стандартом DVB-S, что позволяет экономить на услугах спутникового оператора.

Спутниковый ретранслятор – лишь один из возможных способов доставки сигнала до базовых станций сети. В качестве альтернативы можно использовать, например, арендованные каналы связи на основе различ-

ных транспортных протоколов – как SDH, так и IP/MPLS. Каждый из вариантов имеет свои преимущества и недостатки. Например, наземные сети связи, использующие волоконно-оптические каналы, обладают гораздо большей помехозащищенностью, надежностью, достоверностью при передаче информации. В то же время в случае спутниковой ретрансляции сигнала не играет роли количество базовых станций сети, на которые доставляется сигнал, что является неоспоримым преимуществом с учетом просторов нашей Родины, а во многих случаях сложности организации наземных линий связи вне населенных пунктов.

Сеть передающих базовых станций

Сети DVB-H могут иметь разную топологию. Один из вариантов – использование нескольких сайтов с мощными (несколько киловатт) передающими устройствами на больших высотах. Размещение подобного оборудования обеспечивает обширные зоны покрытия для каждой из станций и хорошее проникновение сигнала «сверху» в кварталы с плотной застройкой, но предъявляет повышенные требования с точки зрения ЭМС и санитарных норм. Соответственно такие передатчики можно располагать только в строго определенных местах, таких как специализированные телевизионные и радиоцентры, трубы ТЭЦ и т.д. Кроме того, при таком способе построения сети могут возникать проблемы ухудшения помеховой обстановки в условиях городской застройки из-за большого количества переотражений сигнала в точке приема.

Второй вариант – использование одного-двух мощных передатчиков, каждый из которых обеспечивает большую зону покрытия, и охват остальной территории с помощью передатчиков средней и малой мощности. Преимущество данной топологии – более равномерный уровень напряженности поля.

Третий вариант – строительство сети на основе однотипных передатчиков средней мощности. Этот вариант позволяет создать равномерное покрытие на всей территории предоставления услуги.

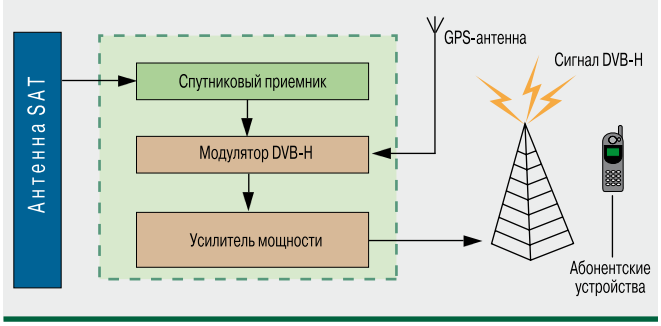
Дополнительный плюс второго и третьего варианта – исключение помехового влияния сигнала мощных передатчиков на большом удалении от них. Размеры зоны обслуживания каждого из передатчиков определяются величиной защитного интервала; этот параметр устанавливает максимальный размер зоны обслуживания каждого передатчика, при котором не проявляется его мешающее влияние на соседние передатчики. В сети компании «Доминанта» выбрано значение защитного интервала 1/8, что соответствует зоне обслуживания примерно 32 км.

Сеть компании состоит из 35 сайтов (рис. 3), в которых располагаются спутниковые ресиверы, принимающие сигнал со спутника, а также передающие устройства, транслирующие сигнал DVB-H, которые обеспечивают покрытие с заданным качеством услуги на 80% территории Москвы в пределах МКАД. Кроме того, в состав базовой станции входят система бесперебойного питания, система дистанционного управления, технологические системы кондиционирования, сигнализации и пожаротушения. Основу вещательной сети составляют передатчики мощностью от 100 до 1000 Вт.

В спутниковом приемнике из полученного потока стандарта DVB-S2 через интерфейс ASI поток MPEG2-TS «извлекается» и пересылается в модулятор DVB-H. Далее происходят модуляция сигнала и его излучение на заданной частоте. Как уже говорилось, для сети «Доминанты» это 514 МГц.

В компании «Доминанта» было принято решение использовать для распространения сигнала DVB-H одночастотную сеть (SFN). В связи с этим для синхронизации всех передатчиков на базовых станциях используются GPS-приемники с выходами 1 pps и 10 МГц. Параметры синхронизации, в том числе задержки распространения до каждой из базовых станций, закладываются, как было сказано выше, в MIP Inserter на головной станции.

Рис. 3. Структура сайта (базовой станции)



Исторически для эфирного телевизионного вещания использовалась горизонтальная поляризация сигнала. Отчасти это связано с тем, что ТВ-антенны коллективного приема располагались на кровлях зданий. Цифровое ТВ стандарта DVB-H в основном рассчитано на то, что пользователи услуги будут находиться примерно на уровне 1,5 м от поверхности земли. В соответствии с этим используется вертикальная поляризация передаваемого сигнала. Конечно, в условиях плотной городской застройки при распространении сигнала поляризация его может меняться из-за множества переотражений сигнала на пути к абонентскому приемному устройству, но с учетом планов дальнейшего расширения территории предоставления услуги за пределы крупных населенных пунктов предполагается, что вертикальная поляризация более перспективна.

Система мониторинга и управления

Система состоит из двух частей, которые отвечают за мониторинг базовых станций и сервисных платформ и за мониторинг головной станции. Мониторинг базовых станций и сервисных платформ происходит по протоколу SNMP с помощью программного комплекса Zabbix. Программный комплекс Lazulite ведет мониторинг состояния головной станции. Обе системы позволяют в реальном времени отслеживать работоспособность оборудования и каналов связи, а также дистанционно управлять ими.

Телефоны для мобильного ТВ

Абонентские устройства

Для приема сигналов мобильного телевидения стандарта DVB-H подходят несколько групп абонентских устройств: телефонные аппараты, автомобильные медиаустройства, GPS-навигаторы и КПК, USB-модемы сетей GSM/3G, медиаплееры и т.д. Эти устройства могут быть оснащены встроенными или иметь внешние приемники DVB-H. В последнем случае устройство представляет собой отдельный приемник DVB-H, совмещенный с точкой доступа Wi-Fi или имеющий интерфейс связи Bluetooth, к которому можно организовать соответствующее соединение с абонентского устройства пользователя для подключения к услуге.

Каждая из групп устройств имеет свои преимущества и рассчитана на определенную потенциальную аудиторию. Одновременное развитие сразу нескольких типов совместимых устройств DVB-H и невысокая стоимость пользования услугой позволит цифровому телевизионному вещанию стать в течение короткого времени достаточно популярным у пользователей.

В настоящее время используются две основные разновидности стандарта DVB-H, различающиеся способами распространения прав на просмотр контента абонентскими устройствами. Обе они реализованы в сети «Доминанты». Разновидность, называемая OSF (IPDC), основана на рассылке сообщений о предоставляемых правах на просмотр программ внутри сформированного транспортного потока TS ASI. Необходимым условием пользования услугой является абонентское устройство с приемником DVB-H, а также SIM- или SD-картой, в которую вложен специальный программный апплет – область данных, являющая частью используемой системы CAS. Апплет проводит сравнение заложенных в нем параметров с принимаемым из эфира сигналом, несущим права на просмотр программ определенным абонентам. У стандарта OSF есть свои плюсы и минусы. К плюсам можно отнести его «независимость» от GSM-сетей, что позволяет применять GSM-независимые терминалы, такие как GPS-навигаторы, КПК, медиаплееры и автомобильные медиаустройства. Как ни парадоксально, независимость от сети сотового оператора в некотором аспекте является минусом. Авторизация в стандарте OSF происходит посредством сети DVB-H, что заставляет привязывать терминал к SIM- или SD-карте. Такая ситуация создает неудобства абонентам сети GSM, поскольку для того, чтобы подключиться к услуге «Мобильное телевидение», им в дополнение к телефонному аппарату с приемником DVB-H придется заменить старую SIM-карту на SIM-карту с апплетом.

Второй стандарт, OMA BCAST, не связан с SIM-картой GSM-оператора, поэтому его можно использовать для расширения клиентской базы за счет абонентов других сотовых сетей. Но он требует наличия обратного канала GPRS/3G, с помощью которого и организуется процесс выдачи прав на просмотр программ.

Сейчас абонентам «Билайн» доступны телефон стандарта OSF – это Samsung SGH-P960 – и модель Nokia 5330 Mobile TV Edition с поддержкой стандарта OMA BCAST (рис. 4). В ближайшее время в продаже появятся и другие модели.

Тестирование сети

На текущем этапе компании «ВымпелКом» и «Доминанта» совместно с ФГУП НИИР, ФГУП ГРЧЦ, ФГУП РЧЦ ЦФО проводят тестирование построенной сети, в котором принимают участие абоненты «Билайн».

Цели и задачи тестовой зоны обозначены следующим образом:

- анализ возможности выдачи разрешений на оказание услуг связи для целей эфирного вещания в стандарте DVB-H на постоянной основе;
- исследование ЭМС РЭС опытных сетей с действующими ТВ-станциями гражданского, военного и специального назначения в Москве и Московской области;
- анализ возможности и условий предоставления контента общероссийских обязательных общедоступных телеканалов операторам мобильного вещания DVB-H;
- исследование влияния сигнала DVB-H на проводные сети телерадиовещания (кабельные);
- анализ характеристик и особенностей использования различных видов абонентских приемных устройств;
- оценка необходимости внесения изменений в действующие нормативно-правовые акты и разработки дополнительных нормативных требований к сетям мобильного вещания DVB-H.

Результаты тестирования показали возможность эксплуатации сетей мобильного телевизионного вещания стандарта DVB-H для оказания услуг эфирного телевизионного вещания на территории Российской Федерации. Существенных ограничений для применения РЭС-сетей стандарта DVB-H совместно с РЭС существующих и планируемых сетей других операторов связи, а также РЭС военного и специального назначения выявлено не было.

Были организованы и дополнительные экспериментальные работы, нацеленные на подготовку рекомендаций по исключению помех в распределительных кабельных сетях. Меры по переносу трансляции телеканалов на другие частоты сетей кабельных операторов признаны достаточными для обеспечения ЭМС широкополосных мультисервисных кабельных сетей. ИКС

Информационная безопасность на новом уровне – тема года для российского телекома

Отрасль связи сегодня развивается очень динамично, и столь же активные процессы идут на рынке решений информационной безопасности для телеком-сектора. Об этом мы беседуем с руководителем направления по работе с телекоммуникационными компаниями Центра информационной безопасности компании «Инфосистемы Джет» Натальей БАТАЛОВОЙ.

Наталья БАТАЛОВА

– Как вы оцениваете отношение к проблемам информационной безопасности в телеком-секторе? Какие тенденции наблюдаете?

– Проблемам ИБ в телекоме уделяется большое внимание, их важность осознают не только руководители технических подразделений, но и бизнес-руководство. Обеспечение должного уровня ИБ причисляют к важнейшим составляющим успешности компании. Проекты активно финансируются, но при условии обоснования финансовой эффективности.

На ситуацию с ИБ в отрасли действуют как внутренние, присущие непосредственно телекоммуникационному бизнесу, так и внешние факторы.

К внешним в первую очередь относится закон «О персональных данных» – операторы массово занимаются такими проектами. Специфика такова, что телеком-компании эксплуатируют, наверное, самые передовые ИТ-инфраструктуры, в составе которых работают дорогостоящее оборудование и критичные приложения, и при этом владеют колоссальным объемом персональных данных. Строгое следование закону для них не только выливается в огромные инвестиции, но и грозит снижением производительности продуктивных сетей и приложений. Ошибки в проектировании систем защиты персональных данных могут стоить слишком дорого! Поэтому мы придерживаемся сбалансированного подхода, основные принципы которого – «не навредить» и «не тратить средства заказчиков только на формальное соответствие, а строить реально полезные системы».

Создаваемый по инициативе лидеров рынка отраслевой стандарт по защите персональных данных призван учесть специфику бизнеса телекомов, сформулировать понятные требования и облегчить прохождение проверок, результаты которых пока не очень предсказуемы.

Основная «внутренняя» тенденция – обострение конкуренции. С целью удержать рынок и привлечь новых абонентов операторы не только стремятся повысить качество базовых услуг, но и работают над запуском дополнительных сервисов, в том числе в области ИБ. Это можно назвать темой 2010 г. в телекоме.

– Как вы оцениваете уровень сервисов ИБ, имеющихся в арсенале российских операторов?

– Пока на рынке присутствуют только базовые услуги, реализация которых несколько разочаровывает. Если в комплекте с домашним Интернетом продается клиентское антивирусное ПО, то говорить об услуге по большому счету нельзя, так как фактически это дистрибуция антивируса, обслуживание которого ложится на плечи абонента. Несколько операторов предлагают услугу «родительский контроль», который позволяет ограничить пребывание ребенка в Интернете по времени суток, но доступ к недетским сайтам контролируется довольно примитивными методами, не дающими надежной гарантии качества. А ведь качество услуг – это основа бизнеса операторов!

Радует то, что серьезные операторы вместе с квалифицированными интеграторами и поставщиками разрабатывают более высокоуровневые услуги ИБ. Некоторые из них уже эксплуатируются в тестовом режиме, так что скоро ожидается их массовый выход на рынок. Мы уже накопили большой опыт таких проектов и сейчас работаем над созданием дополнительных услуг у нескольких операторов. Домашним пользователям предлагается «Чистый интернет» (антивирус), но организованный на стороне оператора, который и гарантирует качество сервиса. Для построения услуги «родительский контроль» применяются сложные многоуровневые средства определения контента, обеспечивающие высокую точность фильтрации.

Сервисы безопасности для корпоративных абонентов в большей степени подбираются под конкретного клиента. Помимо антивируса востребована, например, URL-фильтрация – контроль неделовых коммуникаций, позволяющий компании сэкономить на оплате канала и повысить работоспособность сотрудников.

– Спрос на какие ИБ-сервисы сейчас явно превышает предложение? Какие услуги ожидают своего выхода на рынок?

– Услуга, которая по нашим наблюдениям востребована, но на рынке почти не представлена – защита корпоративных абонентов от DDoS-атак. Многие компании (банки, например) в результате таких атак регулярно теряют деньги. Операторы же только задумываются о реализации такой услуги.

Мы сейчас начинаем работы у нескольких операторов, имеющих большую базу корпоративных абонентов. Услуга недешевая, но клиенты осознают, что ущерб от атаки обойдется на порядки дороже, поэтому прогноз по проникновению и доходности услуги – оптимистичный.

Еще ряд сервисов для корпорантов может «вырасти» из систем ИБ, эксплуатируемых операторами в своих сетях, при наличии достаточных мощностей – в частности, Security Operation Center (SOC) и DLP. Например, оператор может уведомлять абонента об атаке на его сеть или попытке передачи вовне критичных данных и предоставлять инструкции по реагированию. Операторы уже думают о выпуске на рынок целого пласта подобных услуг. Мы как системный интегратор видим значительный потенциал таких проектов.

– Большинство ваших клиентов-операторов – крупные компании национального масштаба. Какими специальными средствами решаются проблемы ИБ в таких компаниях?

– В крупных компаниях, «напичканных» средствами защиты, нереально идти по пути простого их наращивания. Здесь остро стоит вопрос управления и контроля ИБ и оптимизации затрат на эти процессы.

В таких условиях необходимо построение процессов оперативного управления ИБ – мониторинга, управления инцидентами, уязвимостями, полномочиями, соответствиями и др. Реализовать их вручную в крупной компании невозможно, и основным средством автоматизации здесь является SOC – комплекс технических средств, который в совокупности с правильно выстроенными процессами, несмотря на свою высокую стоимость, позволит снизить затраты на управление безопасностью и поддержание ее на требуемом уровне.

Еще один востребованный класс решений – Identity Management (IdM). Они актуальны в компаниях с большим количеством пользователей и систем, в которых пользователям назначаются полномочия (электронная почта, серверы корпоративных каталогов, серверы баз данных, HR-системы и т.д.). Построение IdM-системы – проект не из дешевых, но такая система дает возможность не только навести порядок с полномочиями пользователей, что заметно повышает уровень безопасности компании, но и сэкономить за счет автоматизации ручного труда.

– Какие основные задачи стоят сегодня перед телеком-операторами, и что могут предложить системные интеграторы для их решения?

– Среди главных задач крупных операторов – борьба с мошенничеством и потерей доходов.

Один из основных видов мошенничества, который невозможно побороть стандартными фрод-машинами, – нелегальная терминация трафика. Пилотные проекты, проведенные нами в 2009 г. во всех регионах РФ, показали, что в среднем треть трафика в России «приземляется» некорректно (от 8–10% в небольших райцентрах до 70% в мегаполисах). Потери крупного оператора достигают сотен миллионов рублей в год. С конца 2009 г. мы ведем коммерческие проекты в ряде операторских компаний и можем похвастаться следующими результатами: только за один квартал прирост выручки зонового оператора составил десятки миллионов рублей! Таким образом, за короткий период наши проекты окупаются несколько раз.

Для сокращения потерь доходов из-за некорректной тарификации и других причин (а это 5–20% выручки оператора) используются системы гарантирования доходов (Revenue Assurance, RA). Они стоят достаточно дорого, и для их построения требуется серьезное обоснование. Поэтому сначала мы проводим RA-аудит и оценку потерь (сложная и трудоемкая работа, которую, по моим данным, в России сейчас может квалифицированно выполнить только наша компания) и лишь потом начинаем поэтапное внедрение системы, обеспечивающей в первую очередь защиту наиболее критичных для данного оператора зон риска. При таком подходе система RA, несмотря на высокую цену, способна окупиться в среднем в течение года. Это уже поняли многие мобильные операторы, и теперь дело за их коллегами из сектора фиксированной связи.

У мобильных операторов сейчас идет «волна» активности по защите от смс-фрода: многие подверглись и продолжают подвергаться смс-атакам и терять деньги. Опять же, оптимальный, по нашему опыту, подход – начать с аудита: сделать «срез трафика» и выявить, какие виды смс-фрода имеют место, и тогда решение по защите от него будет экономически оправданным и эффективным.

– В последнее время много говорят о системах предотвращения утечек информации. Насколько актуальны DLP-системы в телекоме?

– Сегодня, наверное, нет компаний, в которых не были бы внедрены элементы DLP. Ведь бывают случаи, когда утечки обходятся в сотни тысяч долларов! И телекомы – не исключение. В зависимости от зрелости DLP-функции у клиента наши проекты различаются: от внедрения базового функционала в течение месяца до создания полномасштабной системы, включая построение процессов контроля утечек, в которые помимо подразделений ИБ вовлечены службы экономической безопасности, HR и др.

В нашем арсенале DLP-продуктов два-три лучших, на наш взгляд, импортных средства и собственная разработка – «Дозор», недавно отметившая свое 10-летие и также обладающая мощным DLP-функционалом. Продукт позволяет контролировать содержимое сетевых ресурсов, сообщений электронной почты, социальных сетей, веб-почты, ICQ, создавать «цифровые отпечатки» с документов. Основные отличия «Дозора» – хорошее «понимание» русскоязычного контекста, высокая точность срабатывания, максимально широкий список контролируемых российских ресурсов и мощная система архивирования и поиска, позволяющая хранить переписку в течение требуемого времени и оперативно извлекать нужную информацию при разборе инцидентов.

Беседовала **Евгения ВОЛЫНКИНА**

Инновационный бизнес = гениальные разработчики + профессиональные продавцы

Так сформулировал правило коммерциализации инноваций Арсений ТАРАСОВ, генеральный директор Siemens Enterprise Communications в России и странах СНГ. С первым слагаемым, по его мнению, в России все в порядке; но вот со вторым – большая проблема, для решения которой требуется вырастить как минимум первое поколение корпоративных продавцов. А в перспективе – создать школу корпоративных продаж сложных продуктов.

Арсений ТАРАСОВ

– Арсений Александрович, в своем блоге в ЖЖ Вы пишете, что для реализации инновационной программы в России крайне необходимы люди, обученные организации продаж как бизнес-процессу. Почему эта задача так актуальна?

– Президент страны говорит о необходимости диверсификации экономики и создания нового экспортного потока выручки с помощью инновационных продуктов – это не может не радовать. И сегодня на этой радостной волне все рассуждают об инвестициях в инновации, о привлечении венчурных фондов, о стартапах, о замечательном технополисе, который у нас будет в Сколково, и т.д. Все правильно и здорово. Но при этом многие – да почти все – забывают о том, что бизнес должен зарабатывать деньги. Собственно, бизнес становится бизнесом именно после того, как компания начинает приносить прибыль, формировать бюджетные поступления, платить налоги и проч. Как это сделать – нигде не рассказывают, никого не учат. Скажем, для реализации хороших амбициозных планов «Роснано» создать к 2015 г. индустрию с оборотом в 900 млрд рублей (почти $30 млрд) потребуется от 5 до 10 тыс. корпоративных высококлассных продавцов, которые будут уметь эту продукцию реализовывать на российском и зарубежных рынках. Посчитать просто: в индустрии инновационных технологических продуктов один корпоративный продавец имеет план в размере в среднем от $5 млн в год (общемировые цифры). В России продавцов такого класса, увы, очень мало. Вопрос, как правильно продавать на конкурентном рынке высокотехнологичную продукцию, у нас никогда не поднимался на уровне государства. В России нет такой профессии, как корпоративный продавец сложных инновационных продуктов, который в идеальном варианте должен быть консультантом по решению бизнес-проблем заказчиков. Я уверен, что продукты у нас будут производиться, но когда встанет вопрос о том, чтобы страна начала получать от них прибыль, мы окажемся перед огромной проблемой. Придется либо приглашать на эти должности «варягов», либо продавать свои продукты за границу по низким ценам, чтобы иностранные партнеры брали на себя функцию продвижения, оставляя себе значительную долю прибыли. Поэтому я настойчиво со всех возможных трибун (в том числе и посредством ЖЖ) призываю профессионалов, которых волнует будущее нашей страны, поддержать мою инициативу, стать наставниками для нового поколения продавцов инноваций и передавать им свои профессиональные знания и опыт.

– Вы читаете курс лекций по коммерциализации инноваций в Физтехе и МГУ, в бизнес-школе «Роснано», читали и будете читать на форуме инновационной молодежи в «Зворыкинском проекте», готовите к изданию книгу "Как вывести инновационный продукт на рынок, или Управление процессом корпоративных продаж сложных продуктов"... Есть первые итоги в деле создания школы продавцов B2B в России?

– Этот проект займет не один год, но, без сомнения, должен принести пользу всем. Опыт общения с молодежью, особенно в «Зворыкинском проекте», вызывает и радость, и грусть: людей с горящи-

ми глазами и блестящими идеями много, но, к сожалению, большинство этих идей и начинаний обречены на фиаско. Просто потому, что ребята не понимают, как этот бизнес дальше продвигать. Россия давно проиграла Западу не в разработке инноваций, которых у нас всегда было достаточно, а в умении продвигать их на рынок. Но мы хотим помочь этим людям стать в дальнейшем успешными бизнесменами. Они, может быть, не принесут миллиардных оборотов, как компания PTC. К слову, очень характерный пример: американская компания Parametric Technology Corporation (PTC) была основана в 1985 г. нашим бывшим соотечественником, профессором из Ленинграда Семеном Гейзбергом. В СССР никто не интересовался его программными разработками, а в США на венчурные деньги он создал компанию, оборот которой за 12 лет достиг $1 млрд. Успех был обусловлен комбинацией инновационной технологической идеи и профессиональной команды продавцов корпоративных решений. Не уверен, что такие миллиардные продукты появятся в результате проектов этих молодых ребят. Тем не менее даже небольшой бизнес – уже успех.

– Кстати, Ваша карьера успешно складывалась в PTC, а до этого в Cisco. Что сподвигло Вас перейти в начале 2009 г. в Siemens Enterprise Communications, которая ассоциируется с традиционной телефонией?

– Вы знаете, что Siemens Enterprise Communications, а также компании Cycos и Enterasys Networks входят в SEN Group – организованное в 2008 г. совместное предприятие американской инвестиционной компании Gores Group и Siemens AG. В SEN меня заинтересовали три важных момента. Во-первых, это громадный, более чем 150-летний опыт Siemens в области технологий передачи голоса, мощная культура разработки продуктов. Во-вторых, это инновационные разработки последних десяти лет плюс привнесение в технологии Siemens сетевых технологий Enterasys. И, что очень важно, новый американский менеджмент, который имеет очень четкие понятные амбиции как на ключевом немецком рынке, так и на других рынках – Северной Америки, Южной Америки, EMEA. Как показывает опыт последних 20–30 лет, чтобы хороший продукт хорошо продавался, должна работать правильно выстроенная команда продаж. В SEN сошлись необходимые слагаемые инновационного бизнеса – хороший продукт и возможность выстроить команду, которая будет заниматься продвижением этого продукта на рынке. Мне очень понравились амбиции этой компании и ее возможности. Создать в России сильного игрока на рынке корпоративных коммуникаций – эта задача мне представляется чрезвычайно интересной.

– Вы упомянули об инновационных разработках SEN – именно на них будет сделана ставка при продвижении продукции компании в России?

– В России первый в мире программный SIP-коммутатор корпоративного класса для крупных предприятий, реализующий задачи унифицированных коммуникаций, Siemens OpenScape Voice и программный коммутатор для малых и средних предприятий Siemens OpenScapeOffice MX впервые были представлены на выставке «Связь-Экспокомм 2010». Незадолго до этого решение унифицированных коммуникаций Siemens OpenScape UC Server 2010 удостоилось награды «Лучшее решение на выставке VoiceCon 2010» и было признано компетентным жюри самым инновационным. Признание VoiceCon 2010 для Siemens Enterprise Communications стало знаковым: впервые компания с более чем 150-летней историей телекоммуникационного производства вышла за рамки имиджа поставщика традиционных телефонных технологий, замахнувшись на «IP-Олимп». Это решение позволяет либо предложить новую услугу, либо выстраивать телефонию в очень крупных масштабах: двух стандартных серверов достаточно для обслуживания 100 тыс. абонентов. Как мы говорим, SEN привела телефонию в ЦОДы.

Уже в июне этого года мы завершили крупный проект на базе Siemens OpenScape Voice на территории СНГ. В настоящее время практически со всеми своими крупными заказчиками компания ведет переговоры либо о пилотных проектах, либо о внедрениях этого решения, которое вызывает большой интерес у крупных предприятий и операторов связи.

– А что будет с продукцией SEN на «Калугаприборе»?

– Конечно, коммутационные системы HiPath 4000 остаются приоритетными для государственных заказчиков. В прошлом году мы отметили 10-летие лицензионного производства Siemens на базе ФГУП «Калугаприбор», открытого в рамках ФЦП по развитию коммуникационных решений для органов государственной власти. Сначала на заводе выпускались станции Hicom 300, а затем HiPath 4000. Причем это не «отверточная» сборка, а производство с глубоким уровнем проработки. Так как «Калугаприбор» является Федеральным государственным унитарным предприятием, его продукция может производиться в так называемом информационно защищенном исполнении и использоваться для нужд российских стратегических сетей связи. Например, среди крупных проектов можно отметить построение сетей связи для саммитов G8 в Санкт-Петербурге в 2006 г. и в Самарской области в 2007 г.; среди заказчиков – силовые структуры, ГТК, МПС, банки и другие организации России и стран СНГ. Могу сказать, что сегодня производство способно выпускать оборудование в объемах, превышающих существующие потребности наших государственных органов по строительству корпоративных телефонных сетей. В настоящее время SEN рассматривает возможность открытия новых технологических линий по производству коммутаторов и телефонов. Вообще сегодня многие вендоры заявляют о намерении открыть локализованное производство в России, однако для этого, на наш взгляд, необходимо опираться на гарантированный спрос «якорного» заказчика, поскольку таможенные пошлины на комплектующие все еще превышают пошлины на готовое изделие.

Беседовала **Лилия ПАВЛОВА**

Почему «не устанавливается» режим коммерческой тайны

Институт коммерческой тайны, возродившийся в нашей стране после длительного (начавшегося в 1917 г.) перерыва, еще очень молод, практика правоприменения пока не наработана. И хотя российское законодательство четко определяет режим коммерческой тайны и мероприятия для его установления, реализация этих мер на предприятиях наталкивается на серьезные препятствия.

Михаил ЕМЕЛЬЯННИКОВ, директор по развитию бизнеса НИП «Информзащита»

Читая интервью и комментарии политиков, бизнесменов, законодателей, постоянно встречаешься с отказом раскрыть те или иные сведения со ссылкой на «коммерческую тайну». Ею объявляют буквально все: размер оплаты труда и наличие счета в оффшорном банке, источники финансирования для закупок компании и сведения о военнослужащих, пропавших без вести во время Великой Отечественной войны, условия размещения оргкомитета Олимпиады-2014 в выбранном офисе и количество дольщиков у обанкротившегося застройщика. Чаще всего такие отсылки – следствие правовой неграмотности. Коммерческая тайна – это вовсе не те сведения, которые знающий их раскрывать не хочет по только ему ведомой причине. Коммерческая тайна, а если быть точным, информация, составляющая коммерческую тайну (и.к.т.), – это строго определенная законом категория сведений. Она имеет три главных признака:

- наличие коммерческой ценности;
- неизвестность на законном основании третьим лицам;
- установление в отношении этой информации режима коммерческой тайны, т.е. особого режима обращения, обеспечивающего ее конфиденциальность.

Нет у информации коммерческой ценности – значит, никакая это не коммерческая тайна, как бы обладателю ни хотелось скрыть ее от посторонних (или общества).

Не установлен в организации режим коммерческой тайны – не может информация считаться таковой, как бы ни была она важна для бизнеса.

Российское законодательство очень жестко и однозначно определяет, что ограничение доступа к информации возможно только на основании федеральных законов. Для коммерческих секретов это IV часть ГК РФ и ФЗ «О коммерческой тайне». В них четко прописано, что и как можно (именно можно, а не должно!) относить к секретам, что представляет собой режим коммерческой тайны и какие мероприятия надо проводить для его установления и поддержания. В случае невыполнения требований закона велик риск не получить помощи от государственных институтов – судов, прокуратуры, правоохранительных органов – в защите исключительных прав обладателя информации, составляющей коммерческую тайну, и привлечении к ответственности виновных в неправомерном доступе к ней.

Практическая реализация режимных мер наталкивается в российских компаниях и организациях на серьезные препятствия, преодолеть которые удается далеко не всегда. В лучшем случае режим формально устанавливается, но существует он только «на бумаге». В худшем случае жить в условиях режимных ограничений становится невозможно, и от него приходится отказаться вовсе.

Требований закона, определяющих содержание режимных мер, всего пять:

1) наличие в организации перечня информации, составляющей коммерческую тайну, утвержденного установленным порядком;

2) ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за его соблюдением;

3) учет лиц, получивших доступ к и.к.т., и лиц, которым такая информация была предоставлена или передана;

4) регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

5) нанесение на материальные носители, содержащие информацию, составляющую коммерческую тайну, грифа "Коммерческая тайна" с указанием обладателя этой информации.

Казалось бы, все достаточно просто. Но дьявол, как всегда, в деталях.

Особенно сложной стала реализация режима после вступления в силу с 1 января 2008 г. IV части ГК РФ, поставившей знак равенства между и.к.т. и секретом производства (ноу-хау). А что делать коммерческим организациям, в которых производства нет в принципе – банкам, страховым компаниям, рекламным агентствам, операторам связи? Весьма расширительное трактование в законе понятия «секрета производства» дает основание полагать возможным отнесение к и.к.т. и иных сведений, не связанных с технологиями.

Верхи не хотят, а низы не могут

Первая и главная проблема – режим коммерческой тайны не устанавливается «снизу». Ни руководитель службы безопасности, ни юрисконсульт, ни главный технолог не могут выступать драйверами процесса установления режима. Защита исключительных прав нужна владельцам

бизнеса и топ-менеджерам, заинтересованным в долгосрочных результатах деятельности компании. Если руководители высшего звена сами не инициируют или хотя бы не поддерживают активно ограничение доступа к коммерческим секретам в рамках режимных мер, попытки установить режим обречены на провал.

Для всего персонала компании при этом надо определить комплекс стимулирующих и мотивирующих мер, иначе все указания «сверху» будут просто саботироваться. Ограничения не удобны никому. За них надо платить – или наказывать за невыполнение ограничительных требований. Лучше делать и то и другое. Но, прежде чем требовать выполнения установленных ограничительных мер, персонал надо обучить правилам их соблюдения. А на этом часто экономят.

Что-то с перечнем не так

Проблемы начинаются с формирования перечня и.к.т. Поскольку не существует общедоступных методик, позволяющих определить, можно ли отнести информацию к и.к.т. и какова ее коммерческая ценность, каждый начинает самостоятельно «изобретать велосипед». Результат представить себе нетрудно. В перечень попадает информация, доступ к которой ну очень хочется ограничить, но к и.к.т. не имеющая никакого отношения (см. выше), или прямо запрещенная к охране в режиме коммерческой тайны законом (особенно популярны здесь сведения об авариях, катастрофах, безопасности производимых продуктов и т.п.), или такая, которую невозможно охранять в режиме коммерческой тайны. Самая распространенная категория последней группы – сведения об оплате труда. Любой работник на законном основании может получить на руки справку о доходах физического лица (форма 2-НДФЛ) и далее использовать ее по собственному разумению – сдать в налоговую инспекцию, представить в банк или просто вывесить на заборе. Попытки со стороны работодателя поставить ограничительный гриф на 2-НДФЛ приведут к оспариванию самой правомерности установления режима коммерческой тайны (часть 8 ст.11 ФЗ «О коммерческой тайне») в отношении этих сведений. И выиграть такой иск работодатель вряд ли сможет.

Вторая распространенная проблема с формированием перечня и.к.т. – весьма расширительное, общее определение категорий относящихся к ней сведений, что не позволяет реально отнести к этой категории те или иные документы. Характерный пример – «договора с контрагентами, содержащие цены поставки продукции (оказания услуг)». Что, все договора? На поставку бумаги для принтеров-ксероксов и косметический ремонт помещений тоже? И в чем же их коммерческая ценность?

Все на защиту секретов!

Как правило, после установления на предприятии режима коммерческой тайны договора о неразглашении секретов срочно заключаются со всеми без исключения работниками. Между тем закон четко определяет, что доступ к и.к.т. предоставляется только тем сотрудникам, которым она необходима для выполнения их трудовых обязанностей.

Крайне живучей оказалась пришедшая из советских времен традиция принуждения работников к подписанию обязательств или «подписок» о неразглашении. Между тем российское законодательство отрицательно относится к попыткам наложения односторонних обязательств на работника, признавая их в судах юридически ничтожными. И действительно, согласия работников на соблюдение режимных требований мало. Для их реализации надо создать необходимые условия для соблюдения конфиденциальности, а это как раз обязанность работодателя.

Защищать все сведения – бессмысленно и дорого. Допускать к и.к.т. всех работников – противоречит закону. Игнорирование этих очевидных постулатов при установлении режима заканчивается крахом.

И дух, и буква закона подталкивают обладателя исключительных прав на секрет производства к тому, чтобы составить конкретный, строго определенный список лиц, имеющих доступ к и.к.т. Со списком возникают постоянные проблемы (текучка!), поэтому оптимальным представляется формирование номенклатуры должностей работников, имеющих соответствующий допуск. И неплохо было бы сразу предусмотреть им денежную компенсацию за установленные ограничения…

Гладко было на бумаге...

Организация работы с конфиденциальными документами обычно не вызывает особых затруднений. Но как только дело доходит до хранения, обработки и передачи информации в вычислительных сетях, ситуация резко ухудшается. Создание разрешительной системы доступа к электронным документам и данным требует не только эффективного управления идентификацией и правами, но и логирования действий администраторов и пользователей. Обязательной становится инвентаризация информационных ресурсов, выявление тех из них, где содержится и.к.т. В качестве обязательных мер напрашивается также мандатное управление доступом и управление электронными правами.

Если мы имеем дело с электронными документами в «офисном» формате, эти проблемы как-то еще решаются. Но при работе с базами данных и сложными приложениями типа СЭД, ERP- или CRM-систем перенос режимных мер в информационную систему становится задачей сложной, трудноразрешимой и очень затратной.

В современной организации документов только в бумажном виде практически не существует, все они создаются на компьютерах пользователей. Поэтому режимные меры, не обеспечивающие защиту и.к.т. в электронном виде, не могут считаться ни разумными, ни достаточными. И снова режим буксует…

■ ■ ■

Тем не менее выгоды, которые получает обладатель исключительных прав на специфические результаты интеллектуальной деятельности – секреты производства, установив в отношении этой информации режим коммерческой тайны, очевидны. Потому «работа над ошибками» будет продолжаться, и на возникающие вопросы придется искать адекватные ответы.

Verimatrix и потоковая передача с адаптивным битрейтом: платное телевидение на распутье

Александр ГИТИН,
региональный директор Verimatrix Россия, страны СНГ и Балтии

Многие операторы уже сегодня обьединяют OTT-сервисы и технологии потоковых передач с адаптивным битрейтом. Платные ТВ-услуги, использующие данные технологии, помогают операторам повысить ARPU, лояльность абонентов и привлечь дополнительные рекламные средства.

Платное телевидение сегодня имеет уникальную возможность сделать шаг вперед: с одной стороны, у операторов есть все необходимое для завоевания новых клиентов и предоставления дополнительных услуг, с другой стороны, пользователям открываются перспективы просмотра контента гораздо более высокого качества на разнообразных устройствах (медиаприставках, персональных компьютерах, смартфонах) через Интернет, сети Wi-Fi, 3G, и все это без привязки к определенному оператору.

Verimatrix в своих решениях по защите и доставке контента использует стандарт H.264, MP4 и технологии Apple. Стандарт H.264/AVC/MPEG-4 Part 10 выбран из-за того, что он содержит ряд новых возможностей, позволяющих значительно повысить эффективность сжатия видео по сравнению с предыдущими стандартами (в частности, ASP), обеспечивая также большую гибкость применения в разнообразных сетевых средах.

Особое место в развитии решений Verimatrix занимает поддержка клиентов для iPhone, поскольку iPhone OS 3.0 (и QuickTime X на других платформах) имеет встроенные средства для обеспечения потоковых передач с адаптивным битрейтом, которые действительно помогают сохранить хорошее качество видео через Wi-Fi, 3G,WiMAX и другие сети с переменной пропускной способностью сетевых соединений.

Линейка продуктов Verimatrix готова помочь операторам сетей создать новые условия для передачи и защиты контента и абонентов. Конечным результатом этого процесса будет более богатый выбор контента, а также времени и места его просмотра. На этом фоне бизнес-модель оплаты ТВ-услуг будет тоже развиваться и перейдет на новый уровень – сегодня платное телевидение находится на распутье.

Verimatrix: (926) 525-7624

ИКС pro технологии

Какой спрос с консультанта?

Александр МАРТЫНЮК,
генеральный директор,
«Ди Си квадрат»

Стоит ли привлекать независимых консультантов к проекту создания/модернизации ЦОДа? А если стоит, то чего от них можно ждать и требовать?

На Западе при выполнении проектов создания и модернизации дата-центров существует распространенная практика привлечения независимых консультантов, компетентных в данной области. Хотя услуги таких специалистов обходятся недешево, инвесторы и владельцы площадок убеждены, что это лучший способ экономии проектного бюджета, учитывая цену устраняемых рисков. Этой логики придерживаются как компании, строящие свой первый дата-центр, так и те, кто уже давно не новичок в этом деле. В России ситуация иная: на ранних этапах проекта мало кто решается делиться информацией с «чужаком» – соблюдают повышенную конфиденциальность, а когда проект закончен и огрехи начинают лезть из всех щелей – тут уж самолюбие не позволяет.

Попробуем разобраться, насколько оправдана такая позиция. Как оценить, что можно выполнить своими силами, а что следует доверить консультанту? И как понять, действительно ли консультант заслуживает доверия или просто пытается «засветиться» на фоне солидного заказчика? Искать ответ мы будем step by step – рассматривая ситуацию на каждой стадии проекта.

Начало проекта: выбираем разработчика проектного решения

Стадия Site Assessment – осмотр площадки под ЦОД: либо на этапе подбора, если речь идет о новом строительстве, либо на этапе подготовки ЦОДа к модернизации. С точки зрения консалтинга этот этап предполагает анализ существующей информации. Речь идет об огромном объеме данных, которые необходимо проанализировать за довольно короткий промежуток времени. Но без этого шага нельзя идти дальше, потому что именно на этом этапе выявляется и устраняется основной объем рисков. А значит, и ответственность за результат этой работы огромная – особенно если речь идет об отказоустойчивом дата-центре, обслуживающем бизнес-процессы, которые должны выполняться в режиме нон-стоп.

Кто может эту работу сделать? Международные консультанты? Нет, они этим не занимаются. Самому заказчику вряд ли имеет смысл браться за решение этой задачи. Для этого необходимо иметь опыт проектирования и строительства дата-центров, и один-два не совсем удачных проекта тут не в счет. Нужно хорошо знать специфику предметной области, разбираться в ее нюансах, хорошо ориентироваться в огромном объеме информации. А для этого требуется команда специалистов-практиков, среди которых есть архитектор, климатик, электрик, энергетик, специалист по слабым токам, специалист по системам пожарной безопасности. Они должны непосредственно на объекте оценить объем работ и вероятность рисков. Если речь идет о модернизации существующей площадки, следует также выполнить анализ проектной документации. Иными словами, на стадии Site Assessment по сути выполняется полноценная техническая экспертиза.

Если заказчик может себе позволить держать в штате такую высококвалифицированную команду (например, он постоянно строит новые дата-центры или обновляет действующие), тогда другое дело. Но, как правило, компании сосредоточены на своем бизнесе. Реализовав один-два проекта создания/модернизации/расширения дата-центра, они эксплуатируют технологическую площадку в течение нескольких лет и держать непрофильных сотрудников им нет никакого резона.

Поставщиком такой услуги может стать и инженерная компания, и проектная группа, и команда, сформированная из сотрудников системного интегратора, и собственно представители консалтинговой компании. Важно одно – работа должна быть доверена компетентным специалистам; уровень компетенций имеет здесь наивысший приоритет. К тому же обязательно – опытным практикам, которые буквально «кончиками пальцев» чувствуют проблему. Выезжая на объект, они способны за считаные часы все тщательно исследовать, обсудить особенности предстоящих работ и выстроить план реализации проекта. И заказчик, и проектировщики, привыкшие работать в офисе, могут упустить из виду многое из того, что видят и понимают опытные инженеры-практики, – они просто не представляют себе всего комплекса задач в объеме.

Чтобы не ошибиться с выбором такой команды, заказчик должен сформировать у себя координирующий центр, в который обязательно должны войти специалисты, разбирающиеся в вопросе. Это может быть как штатный сотрудник, так и приглашенный представитель: консультант, сотрудник системного интегратора... Важно, чтобы этот координационный центр не был прямо или косвенно заинтересован в сотрудничестве с данной компанией.

Важно также, чтобы общение с теми, кто заявляет о своей компетентности, проходило вживую, а не по видеоконференцсвязи или в режиме виртуальных

совещаний. Даже если речь идет о международной команде – люди должны найти время, чтобы приехать, своими ногами и глазами досконально исследовать площадку, а также максимально убедительно подтвердить свои компетенции. Среди доводов обязательно должны быть примеры реальных проектов: «Вот так было – так стало. Наше участие заключалось в выполнении таких-то работ. Вот спецификации. План расстановки оборудования. Энергопотребление. Исходный и итоговый PUE. Это температурно-климатические модели. Вот предложенные нами альтернативные варианты проекта: один – позволяющий извлечь максимум возможностей из существующей ситуации с учетом постановки задачи заказчиком, другой – средневзвешенный вариант». Для проектов модернизации площадки сведения о PUE должны присутствовать в обязательном порядке. Хорошо, если будут расписаны шаги по каждому этапу: температурно-климатическая модель, варианты расстановки оборудования с учетом энергоемкости стоек, PUE и т.п. Понятно, что дилетанту такая работа не по силам: она требует практических навыков, специального программного обеспечения.

Запуская дата-центр в эксплуатацию, надо понимать, что через два-три года необходимо провести аудит текущей ситуации – т. е. снова пройти стадию Site Assessment.

Предпроект: готовим проектное решение

Basic of design – это этап, на котором определяются основные инженерные решения, бюджет и ориентировочные сроки строительства. Что главное на этом этапе? Знание деталей и непредвзятость исполнителя. Если этим пренебрегают, не стоит потом сетовать на то, что в проектном решении заложена чрезмерная избыточность, что бюджет, да и сроки, по ходу реализации проекта выросли сверх всякой меры. И надо четко понимать, что компания, хорошо выполняющая проекты оптимизации вычислительных ресурсов и платформ, отнюдь не всегда обладает необходимыми компетенциями для квалифицированного строительства или оптимизации дата-центра. Слишком уж разная здесь специфика. Если уж заказчик принципиально хочет обойтись без консультанта, то оптимальным выбором может стать инженерная компания с хорошей репутацией и квалифицированным персоналом по каждому из разделов проекта, либо мультивендорный системный интегратор, на счету которого уже есть несколько успешных проектов и в штате которого опять-таки есть люди с опытом управления строительством инженерно сложных объектов и их эксплуатации. За рубежом такую работу нередко передают консультационному отделу инженерной компании.

Чего может заказчик ожидать от этой работы? Вопрос не праздный, учитывая, что в России не сложилась еще культура спроса-предложения на данный вид услуг – каждый поступает в соответствии со своими представлениями и сведениями, почерпнутыми из разных, не всегда достоверных, источников. И это можно считать камнем в огород недобросовестных консультантов и проектных команд, которые, к сожалению, пытаются сделать себе имя на дефиците знаний, в итоге ставя заказчиков в еще более затруднительное положение. Что касается непредвзятости, здесь логика тоже довольно прозрачна. Если проектировщик и исполнитель проекта прямо или косвенно заинтересованы в продвижении решений определенного вендора (поставщика строительных материалов, климатических систем, энергетики...), соблазна им не избежать.

Итак, что должен получить заказчик по окончании стадии предпроекта? Точное техническое описание того, что будет построено под его задачи, – с финансовыми деталями и прогнозами, с календарным планом-графиком, с четкими рекомендациями относительно параметров инженерных решений и вариантов реализации этих решений. Особое внимание необходимо уделить разделам отчета, связанным с инфраструктурой каналов связи и энергообъектов. В них должны быть аналитические выкладки по особенностям площадки с учетом ее масштабов, пропорций, возможных рисков, специфики соседних помещений (сверху, снизу, за стенами), а также прилегающих к зданию дата-центра территорий и расположенных рядом объектов.

В том случае, когда предпроект ведется в связи с подготовкой дата-центра к модернизации, в обязательном порядке должны быть представлены расчеты PUE. Заказчик должен иметь четкое представление о том, какое инженерное оборудование остается, что будет заменяться; во сколько это обойдется и когда окупится в лучшем и худшем случае; каким будет экономический эффект. Чтобы это показать в явном виде, недостаточно красивой презентации в десяток слайдов. Это должен быть серьезный, проработанный документ страниц на 70, в котором обязательно будут разделы, содержащие структурные схемы и базовые параметры систем электроснабжения и охлаждения, поэтажный план зон расстановки оборудования, привязка к конкретной архитектуре, достаточно подробное описание вспомогательных помещений, основных процедур работы систем, особенностей их обслуживания и т. д. Кроме того, составляется план-график с указанием того, в какой последовательности должны выполняться разделы проекта и реализовываться укрупнения, когда и какого типа оборудование можно заказывать, учитывая его сложность и сроки поставки.

По времени этот этап, как правило, занимает несколько месяцев, потому что объем выполняемых работ – фактически львиная доля стадии «П» («Проект»). Не хватает только названий конкретных марок и моделей решения. Ясно, что, пока готовится проект, оборудование заказывать нельзя, но уже можно

DEPO Computers рекомендует подлинную ОС Windows Server® 2008 R2

DEPO Storm 3300P1

Платформа для виртуализации серверов

Одноюнитовый двухпроцессорный сервер DEPO Storm 3300P1 используется в комплексных IT-решениях DEPO для создания ферм виртуализации серверов, занимающих минимальный объем в стойке и обладающих высокой производительностью и отказоустойчивостью. Современные технологии позволяют получить решение, сбалансированное по параметрам производительности, энергопотребления и тепловыделения.

- Предустановленная ОС Windows Server® 2008 R2
- 1 или 2 процессора Intel® Xeon® 5500/5600 серии
- До 96 Гб оперативной памяти DDR3 1333/1066/800MHz ECC
- До 4 жестких дисков SAS емкостью до 600 Гб или SATA емкостью до 2 Тб с «горячей» заменой
- Слоты расширения 2xPCI-E x8
- Встроенный модуль удаленного управления IPMI 2.0 с поддержкой KVM over LAN
- Блок питания 650 Вт с «горячей» заменой
- Форм-фактор 1U, набор для монтажа в стойку в комплекте
- Гарантийные планы от 3 до 5 лет с возможностью обслуживания на месте эксплуатации

Windows Server 2008 R2

Microsoft

от 97 999 руб.

Компания DEPO Computers
комплексные IT-решения • системная интеграция • компьютерные системы
тел. (495) 969-22-22, www.depocomputers.ru

Товар сертифицирован. Реклама

МЫ ИХ СДЕЛАЛИ! ДЛЯ ВАС!

определяться с его поставщиками, потому что все достаточно понятно: основные системы обозначены, архитектура определена, описаны интерфейсы взаимодействия систем, даны необходимые сведения о параметрах управления системами, приведены требования по энергоэффективности, подсчитан достижимый уровень PUE, определены номинальные параметры инженерной инфраструктуры.

Наличие такого документа обеспечивает заказчику высокую детализацию и прозрачность дальнейшего проекта, при том что опытная команда определяет ключевые параметры проекта – деньги и время – с погрешностью не более 30%. Поэтому стоит ли удивляться, что команда, которая со всей ответственностью берется за такую работу, болезненно реагирует как на предложение сделать ее бесплатно в качестве тестового задания, так и на вольные коррективы принятого плана ведения проекта, что нередко случается при выборе в качестве управляющей компании некомпетентного партнера. Даже системные интеграторы, долгое время «зашивавшие» стоимость консалтинга в бюджет последующих работ, все более настоятельно позиционируют подготовку предпроектной документации как предмет отдельного контракта.

Проект: переходим от планирования к действию

Итак, стадия практической реализации проектного решения. Здесь консалтинговая составляющая выражается в наличии внешнего технического контроля, помогающего генподрядчику избежать ошибок, и в работе представителей вендоров, демонстрирующих соответствие своих решений требованиям, отраженным в предпроектной документации.

Технический контроль необходимо рассматривать как отдельную услугу, которая предоставляется управляющей компанией. Функции последней логично закрепить за разработчиком предпроектной документации, досконально изучившим и объект, и особенности заказчика. Это позволит сэкономить время и избежать дополнительных согласований, сверок и прочих рабочих моментов. Управляющая компания является ответственным представителем со стороны заказчика, берет на себя заботы о выстраивании продуктивного взаимодействия между субподрядчиками, о контроле объемов и сроков поставок, о решении многочисленных административных вопросов с внешними инстанциями. т. е. все рутинные вопросы она замыкает на себе, предоставляя заказчику возможность не сильно выходить из привычного ему режима ведения бизнеса на время проекта (примерно год). Управляющая команда (5–9 человек) может быть как внешней, так и внутренней, если бизнес заказчика позволяет постоянно загружать таких специалистов работой. Возможен вариант смешанной управляющей команды – из персонала заказчика и внешнего поставщика консалтинговых услуг. Выбор всегда есть. Главное, чтобы эта проектная команда не была финансово или организационно зависима ни от вендоров, ни от подрядчиков.

Отдельного внимания заслуживает организация поставок оборудования, которое должно прийти не позже положенного срока, но и не раньше, чтобы избежать простоев и сложностей, связанных с ненадлежащим хранением. От грамотной транспортировки зависит, будет это оборудование работать как положено или придет в негодность еще в дороге. Еще один важный момент: учитывая объемы закупок и высокую конкуренцию, этот этап позволяет получить хорошие скидки и выгодные условия технического сопровождения со стороны вендоров или их партнеров на местах. Это возможно, если представитель заказчика хорошо ориентируется в ценовой политике и ассортименте вендора, знает, где речь идет о скидках на готовое к работе решение, а где – только на определенную конфигурацию, которая в данном проекте не нужна. Когда заказчик решает для себя вопрос, покупать ему такую услугу консультанта или нет, имеет смысл сопоставить сумму контракта с возможными складскими издержками, упущенной выгодой по причине сорванных сроков, затратами на доукомплектацию и оформление срочных допоставок.

Даже если заказчик тесно работает с кем-то из вендоров как дистрибьютор, он должен понимать, что заказать партию – привезти ее – разместить – продать – заказать новую – это вовсе не то же самое, что обеспечить доставку оборудования определенной конфигурации к определенному сроку в определенное место. В одном случае он выступает как коммерческий посредник, который заинтересован в большей сумме сделки, а в другом – как конечный потребитель, которому важнее сэкономить и при этом получить максимально выгодные условия поставки и сервисного сопровождения. Группа, контролирующая вопросы логистики, должна обеспечить наиболее оперативное реагирование сервисной бригады на любую поломку. И пусть даже в сопроводительной документации на инженерное решение прописан гарантийный срок работы без аварий 5–10 лет, нештатные ситуации исключать не стоит – ведь речь идет о дата-центре, внеплановая остановка которого чревата серьезными проблемами для бизнеса.

В этой ситуации важно, чтобы консультант со стороны вендора был готов пойти на определенные уступки по цене и убедительно продемонстрировал, что предлагаемое его компанией решение наиболее верное для данного проекта. Одним из факторов убеждения может стать знакомство потенциального клиента с результатами использования аналогичного решения в действующем дата-центре. Оптимально, если удастся посмотреть несколько зарубежных примеров реализации и сравнить два-три аналогичных решения от разных вендоров. Рекомендации относительно возможных поставщиков должны содержаться в предпроектном отчете. Вендор же, в случае его дальнейшего участия в проекте, может порекомендовать и подрядчика, и сервисную компанию, в компетентно-

сти которых он уверен. Будет, кстати, и обсуждение вопросов страхования рисков. С одной стороны, в процессе переговоров станет понятно, насколько надежен ваш потенциальный партнер, а с другой – есть вероятность дополнительного снижения затрат заказчика как на этапе реализации проекта, так и в ходе эксплуатации дата-центра.

От чего хотелось бы предостеречь на этапе выбора подрядчика? Не стоит покупать оборудование у одних, а монтаж доверять другим. Это крайне порочная практика, и проблемы на этапе эксплуатации будут почти наверняка.

Проект закончен. Что теперь?

Запуская дата-центр в эксплуатацию, надо понимать, что через два-три года необходимо провести аудит текущей ситуации – т. е. снова пройти стадию Site Assessment. За это время и сама площадка претерпит определенные изменения, и рынок решений для дата-центров шагнет вперед, сменится несколько поколений ИКТ-систем. Конечно же заказчик будет в курсе основных трендов, но не настолько глубоко, чтобы диагностировать полный спектр рисков и потенциальных улучшений в дата-центре. Для этого нужен опыт постоянного участия в подобных аудитах, отработанная практика квалифицированной подготовки предложений, соответствующее оборудование и все то, о чем шла речь в начале статьи. У заказчика всегда есть свобода выбора команды, которой он может поручить эту работу. В редких случаях это собственный персонал, если компания сумела соответствующим образом выстроить свою кадровую политику. Но более вероятно, что на роль аудитора будет приглашена внешняя консалтинговая команда, к выбору которой снова следует подойти ответственно – как будто в первый раз. И принять во внимание прошлый опыт.

Одним из важнейших профессиональных качеств партнера-консультанта является сочетание широкого бизнес-кругозора, позволяющего понять специфику конкретного заказчика, с хорошим знанием практической проблематики всех составляющих понятия «дата-центр». Хороший консультант не столько говорит, сколько делает – и демонстрирует свою готовность приступить к делу практически сразу, как только он понимает суть задачи и объем предстоящих работ. Надеюсь, что рекомендации, приведенные в статье, станут для читателей своеобразным фильтром, помогающим, с одной стороны, определить собственные задачи и возможности, а с другой – компетентность потенциального партнера-консультанта. ИКС

Топливные элементы в системе резервного электроснабжения базовых станций

Евгений ВИШНЕВСКИЙ, технический директор United Elements, канд. техн. наук
Михаил САЛИН, ведущий инженер отдела исследований и развития United Elements
Владимир ГУМИНСКИЙ, заместитель генерального директора «Премиум Комфорт»
Николай КОРСАК, технический директор «Премиум Комфорт»

Телекоммуникационные компании, находясь на острие прогресса, одними из первых обращают внимание на инновации. Одно из перспективных сегодня направлений – альтернативная энергетика, в частности водородная. Система на водородных топливных элементах в этом году успешно прошла испытания в качестве источника бесперебойного питания базовой станции сети сотовой связи.

Понятие «зеленые технологии» постепенно входит в нашу жизнь. Основными критериями «зеленого проекта» считают эффективное использование энергии, снижение выбросов, высокий уровень безопасности и комфорта. Водородные топливные элементы (ТЭ) – одна из самых экологически чистых технологий: в реакции участвуют только водород и содержащийся в воздухе кислород, а продуктом реакции является водяной пар. Благодаря отсутствию движущихся деталей ТЭ работают практически бесшумно. Кроме того, телекоммуникационное оборудование может функционировать и без механического охлаждения, что исключает утечки фреона. Эти и другие преимущества ТЭ по сравнению с АКБ и ДГУ привели к быстрому распростране-

нию водородных технологий по всему миру, особенно в сфере телекоммуникаций.

В России проблемы экологии пока стоят далеко не на первом месте, однако по мере роста стоимости энергии энергоэффективные технологии становятся все более актуальными. В свою очередь, плохая инфраструктура и низкая надежность электроснабжения на периферии также заставляют обращаться к альтернативным источникам энергии. Примером экологического подхода может служить первая в России БТС с энергоснабжением от солнечных батарей (Краснодарский филиал ОАО «ВымпелКом», гора Чубатая). Пиковой мощности этих батарей хватает для электропитания самой станции и кондиционера, а также для подзарядки аккумуляторов, от которых станция работает ночью. В качестве дополнительного источника электропитания в неблагоприятных погодных условиях предусмотрен дизель-генератор. Этот проект доказал, что в сложных условиях применение нетрадиционных источников энергии уменьшает затраты на строительство и его сроки. Прокладка просеки и строительство ЛЭП от поселка Молдовановка до базовой станции заняли бы около двух лет и потребовали $400 тыс.

Перспективный проект был реализован прошлой зимой и на базовой станции Санкт-Петербургского филиала ОАО «ВымпелКом». Были проведены испытания электропитающей установки (ЭПУ) на водородных топливных элементах, системы естественного охлаждения и специального программного обеспечения для дистанционного мониторинга комплекса оборудования. В ходе испытаний ставилась цель подтвердить работоспособность альтернативной системы бесперебойного питания и установки естественного охлаждения.

Альтернативная система бесперебойного питания

Для проведений испытаний параллельно со штатной системой питания была смонтирована система питания 48 В на основе водородных топливных батарей Dantherm Power. Два водородных ТЭ мощностью по 1,6 кВт и выпрямитель с блоком суперконденсаторов, как показано на рисунке,

Стойка с топливными элементами Dantherm Power

размещаются в 19-дюймовой стойке. Внутри стойки также располагается блок управления и безопасности ЭПУ. Важной особенностью ТЭ Dantherm Power является воздушная система охлаждения топливных элементов. В целом получается очень компактное и надежное решение, которое не боится низких температур, так как охлаждение обеспечивается только за счет вентилятора. ТЭ можно устанавливать в одном помещении с телекоммуникационным оборудованием, поскольку избыточное тепло удаляется через воздуховод отработанного воздуха. Подвижные детали имеются только в вентиляторе, так что цена сервиса для водородной установки будет невысока.

Водородная ЭПУ может работать одновременно в качестве источника бесперебойного и резервного питания для всех потребителей БТС. Суперконденсаторы (ионисторы) предназначены для компенсации кратковременных провалов напряжения. В ходе испытаний они обеспечивали надежную работу оборудования связи базовой станции в режиме частого включения и отключения электроснабжения от городской сети в течение 10 мин с интервалом 30 с. Очень важным достоинством суперконденсаторов является их высокая надежность и большой срок службы – практически неограниченное число циклов заряд-разряд без ухудшения характеристик. В отличие от АКБ, суперконденсатор имеет более широкий диапазон рабочих температур – от –40 до +75°С. Учитывая тот факт, что топливные элементы способны работать при температуре в помещении от 0 до +60°С, появляется возможность изменения температуры внутри БТС, что дает большую экономию ресурса кондиционера и электроэнергии.

Вспомогательными элементами установки можно считать баллоны, расположенные в шкафу снаружи БТС, и газовую арматуру водородных линий. В отличие от аккумуляторных батарей, шкафу с баллонами не требуется специальная система охлаждения или подогрева. Для удобства замены восемь баллонов были разделены на три группы. Каждый 40-литровый баллон после заправки содержит 6 Нм^3 водорода под давлением 150 бар. Учитывая, что для производства электроэнергии требуется около 0,9 Нм^3/кВт·ч, полностью заправленного баллона было достаточно для бесперебойной работы в течение 6 ч всего телекоммуникационного оборудования базовой станции и заградительных огней. В Петербурге замена пустых баллонов на заряженные не составляет проблемы, ее проводят организации по снабжению техническими газами. Основное требование техники безопасности заключается в том, чтобы все работы по замене баллонов проводились персоналом с удостоверениями на право обслуживания сосудов под давлением. Если аттестованные работники

Представляем новую серверную комнату, которая полностью готова к эксплуатации

Интегрированная система охлаждения APC обеспечит наиболее экономически эффективную адаптацию вашей серверной комнаты в соответствии с любыми будущими потребностями

Стоечные системы охлаждения APC забирают горячий воздух с тыльной стороны, в месте его образования, и затем предоставляют охлажденный воздух, готовый для использования в соседних стойках, с фронтальной стороны.

Ваша серверная комната становится барьером на пути внедрения новых технологий?

Консолидация, виртуализация, конвергенция сетей, блейд-серверы — все эти новые технологии повышают эффективность, сокращают затраты и позволяют вам добиваться большего меньшими усилиями. Но они также связаны с проблемами высокой энергетической плотности, охлаждения и управления, которые никогда не учитывались при проектировании традиционных серверных комнат. Вы опираетесь на собственную интуицию, надеетесь на возможности системы кондиционирования здания, или внедряете какие-либо временные решения. Знаете ли вы, как без лишних затрат повысить уровень надежности и эффективности управления в вашей серверной комнате?

Компания APC by Schneider Electric представляет комплексное решение для серверной комнаты

Теперь вы можете получить в рамках одного полнофункционального интегрированного решения все необходимые компоненты электропитания, охлаждения, мониторинга и управления, которые отличаются исключительной простотой внедрения. Все компоненты предварительно протестированы для обеспечения наиболее эффективной совместной работы, и при этом могут органично интегрироваться в ваше существующее оборудование. Вам нужно лишь установить это проверенное и готовое к эксплуатации решение — при этом не нужно оптимизировать конфигурации системы охлаждения или проводить дорогостоящую реконструкцию.
Модульная конструкция с возможностью наращивания ресурсов по мере необходимости дает 100-процентную уверенность в том, что ваша серверная комната будет эффективно работать при любых изменениях ваших будущих потребностей.

Легко и экономически эффективно подготовьте вашу серверную комнату для решения задач будущего

APC избавит вас от трудностей, связанных с поиском оптимальной конфигурации серверной комнаты. Независимые блоки охлаждения InRow, шкафы NetShelter с поддержкой высокой энергетической плотности и системы изоляции воздушных коридоров APC могут быть объединены для создания надежной экосистемы ИТ практически в любой среде. Датчики для мониторинга уровня стойки, встроенные в блок охлаждения автоматизированные элементы управления и интегрированные средства программного управления обеспечивают полный дистанционный контроль и полное представление о состоянии системы. Просто установите устройства защиты электропитания (например, лучшие в своем классе ИБП Smart-UPS или Symmetra), и вы получите полнофункциональную систему для решения текущих и будущих задач.

Если у вас имеется выделенное ИТ-пространство...

Получите готовую систему охлаждения как единое решение с поддержкой высокой энергетической плотности.

Система APC InRow SC, объединяющая блок прецизионного охлаждения InRow SC (охлаждающая способность до 7 кВт), шкаф NetShelter SX и систему изоляции воздушных коридоров Rack Air Containment, предлагается со специальной скидкой (срок действия предложения ограничен). Номера артикулов: RACSC101E, RACSC112E, RACSC201E.

Если у вас нет выделенного ИТ-пространства...

Представляем шкаф NetShelter CX:
компактные серверные шкафы с отличной шумоизоляцией, разработанные для открытых офисных сред.

В этих решениях компоненты электропитания, охлаждения и управления интегрированы в защищенном, бесшумном и охлаждаемом шкафу, дизайн которого отлично сочетается с любой офисной мебелью.

Загрузите **БЕСПЛАТНО** информационную статью APC №68 «Электропитание и охлаждение при использовании питания по Ethernet (PoE)» и **станьте участником розыгрыша* — выиграйте планшетный компьютер iPad.**

Зайдите на сайт **www.apc.com/promo** и введите код **79145t**

APC by Schneider Electric

APC by Schneider Electric в Москве: 119334, Москва, 5-й Донской проезд, д. 21-Б, стр. 10. Тел.: + 7 495 916-7166, Факс: + 7 495 620-9180, Центр поддержки клиентов: +8 800 200 2722, E-mail: apcrustech@apc.com

соблюдают известные им правила, можно не беспокоиться по поводу эксплуатации водородной системы (в том числе баллонов). Герметичность самих баллонов очень высока, для стандартного баллона 50% емкости теряется через 95 лет с учетом максимально допустимой утечки. Что же касается газопроводов, то специальный клапан безопасности автоматически перекрывает водородные линии при их разгерметизации – срабатывает реле давления.

В ходе испытаний работа установки Dantherm Power проверялась в следующих режимах:

- самодиагностика оборудования;
- работа БТС от городской сети электроснабжения;
- работа БТС от водородных элементов в автономном режиме.

Режим самодиагностики необходим не только для проверки работоспособности всех систем ЭПУ, но и для поддержания номинального напряжения на ионообменной мембране. Для топливных элементов с полимерной мембраной характерна ее деградация из-за загрязнения поверхности примесями в водороде. Если выходное напряжение начинает снижаться, то программа контроллера установки Dantherm Power выдает сигнал на клапан продувочной линии, клапан открывается и загрязнения удаляются из топливного элемента. Благодаря непрерывному контролю состояния мембраны ТЭ могут работать с номинальными характеристиками до 4000 ч без перерыва, а срок службы установки составляет более 10 лет.

Испытания показали, что установка успешно выполняет самодиагностику и поддерживает на выходе напряжение DC-48V при работе как от городской электрической сети, так и от водородного элемента в автономном режиме. Система мониторинга топливных элементов фиксирует все изменения контролируемых параметров и аварийные сигналы, а также позволяет контролировать эти параметры дистанционно.

В ходе испытаний к установке было подключено оборудование RBS900/1800, 3G, транспортный узел PPC, заградительные огни и кондиционер. При включении компрессора кондиционера сработала защита установки Dantherm Power от перегрузки. Было принято решение об отключении сплит-системы и подключении установки естественного охлаждения Nordic Blue. При повторных запусках система альтернативного бесперебойного электропитания и оборудование системы мониторинга работали в штатном режиме. В ходе испытаний было проверено и подтверждено соответствие нормативам по обеспечению бесперебойной работы телекоммуникационного оборудования RBS 900/1800 – 4 ч, PPC – 24 ч, заградительных огней – 48 ч.

Помимо проблем экологии, плохая инфраструктура и низкая надежность электроснабжения на периферии также заставляют обращаться к альтернативным источникам энергии

Система естественного охлаждения

Испытания показали, что мощности 3,2 кВт становится недостаточно, если в качестве источника холода используется сплит-система. С другой стороны, если в базовой станции отсутствуют аккумуляторные батареи, то кондиционер в ней необязателен. В случае эффективной теплоизоляции контейнера базовой станции часто случается, что необходимо снимать теплоизбытки, когда температура наружного воздуха существенно ниже температуры внутри станции. В ходе испытаний для снятия теплоизбытков от телекоммуникационных стоек использовали установку Nordic Blue холодопроизводительностью 5,8 кВт. Система естественного охлаждения обеспечивает 0,8 кВт холода на каждый градус разницы наружной и внутренней температуры. Максимальный расход электроэнергии летом (только на вентилятор) составляет 300 Вт. Для сравнения: холодопроизводительность штатной сплит-системы составляет 3,5 кВт при потреблении 1,25 кВт электроэнергии.

Вообще говоря, использование комфортных кондиционеров для охлаждения телекоммуникационного оборудования не выдерживает критики с профессиональной точки зрения. Ресурс лучших сплит-систем составляет не более 36 тыс. ч, соответственно после пяти лет эксплуатации кондиционеры необходимо заменять. По требованиям надежности на базовой станции устанавливают две сплит-системы, причем оба кондиционера вместе со стоимостью монтажных работ, блоком ротации и низкотемпературными комплектами обходятся практически в ту же цену, что и система Nordic Blue. Помимо низкого энергопотребления система естественного охлаждения имеет то существенное достоинство, что она использует постоянный ток 48 В и может бесперебойно работать от аккумуляторов. При низкой наружной температуре установка работает в режиме рециркуляции с нагревом воздуха от встроенного ТЭНа. Нагревательный элемент управляется контроллером, поэтому в холодный период экономия электроэнергии тоже оказывается существенной по сравнению с традиционными обогревателями.

Многие зарубежные операторы сотовой связи в целях сокращения расходов на кондиционирование поднимают уставку температуры внутри базовых станций до +35°С. Проведенные в Европе исследования показали, что такое повышение температуры не влияет на надежность и срок службы

телекоммуникационного оборудования. При использовании аккумуляторных батарей гораздо рациональнее поддерживать температуру +18...22°С не во всем помещении, а только для батарей. Повышение уставки на один градус обеспечивает экономию за счет потребления электроэнергии системами кондиционирования на 7%. Крупнейший в мире по обороту средств оператор связи Vodafone в последние годы провел мероприятия по увеличению температуры на десятках тысяч своих БТС.

По данным СНиП 23-01-99 «Строительная климатология», летняя температура обеспеченностью 0,99 для всех регионов России не превышает указанную уставку. Для населенных пунктов, расположенных в зоне умеренного климата, даже абсолютная максимальная температура воздуха будет ниже +35°С. Таким образом, в нашем климате можно и нужно использовать наружный воздух для охлаждения помещения БТС. Операторы сотовой связи в странах с более жарким климатом уже имеют большой позитивный опыт внедрения фрикулинга. Например, у Vodafone более 40% базовых станций в Великобритании, Ирландии, Германии (даже Португалии и Франции) в последние годы были переведены на режим естественного охлаждения.

■ ■ ■

Итак, в ходе испытаний установки Dantherm Power были подтверждены заявленные производителем характеристики, сбоев и отказов элементов установки не было. Получен положительный опыт монтажа и эксплуатации оборудования с использованием водородного топлива. Работа не представляет проблем при соблюдении требований техники безопасности.

Альтернативная система электропитания на топливных элементах в состоянии заменить целый комплекс оборудования: ИБП, множество аккумуляторных батарей и резервный дизель-генератор. В отличие от аккумуляторных батарей, продолжительность работы топливного элемента в основном зависит от запаса водорода. У водородной системы не существует проблемы перезарядки и саморазряда, что гарантирует стабильность энергетических параметров, упрощает эксплуатацию и хранение резервного источника электропитания. При отказе от аккумуляторов появляется возможность использовать фрикулинг в течение всего года, значительно снижается потребляемая базовой станцией мощность. Это позволяет уменьшить установленную мощность электропитающей установки, улучшает эффективность систем электроснабжения и кондиционирования и тем самым увеличивает надежность работы всей базовой станции. ИКС

Обслуживание оптических разъемов в корпоративных сетях

Денис МОРГУНОВ, менеджер по развитию бизнеса, департамент оптических компонентов и систем HUBER + SUHNER AG

При эксплуатации кабельной проводки оптические разъемные соединители, подверженные внешним воздействиям, оказываются одним из слабых звеньев цепи. Однако часто технический персонал не уделяет им должного внимания. Визуальный контроль состояния поверхности ферула особенно важен, так как удаление посторонних включений из порта оптического трансивера требует больших усилий, а зачастую и вовсе невозможно.

Контроль состояния поверхности ферула оптического разъемного соединителя играет важную роль, поскольку прямые и обратные потери зависят от типа механического повреждения волокна и наличия посторонних частиц в зоне контакта. Однако вопрос о том, какова требуемая степень чистоты поверхности ферула, вызывает споры в профессиональном сообществе. Необходимо отметить, что контроль и чистка разъемных соединителей – это дополнительные расходы при производстве и монтаже волоконно-оптических компонентов. Поэтому зачастую возникает противоречие между требованиями потребителя и производителя компонентов и ухудшается соотношение цена/качество изделия.

Наиболее распространенным способом контроля является визуальный, при помощи портативных оптических микроскопов или видеосистем. При выборе оборудования визуального контроля необходимо учитывать целый ряд параметров, таких как коэффициент увеличения, освещенность, разрешающая способность системы, способность распознавать дефекты разного происхождения.

Так, коэффициент увеличения определяет, насколько оптическая система способна зрительно приблизить объект. Освещенность существенным образом влияет на качество изображения объекта. При освещении торца соединителя сила отражения от поверхности оптического волокна и от поверхности керамического ферула будет разной, что затрудняет получение четкой равномерно освещенной картины. Существует несколько методов – с высокой и низкой освещенностью, с изменяемым интерференционным контрастом, в поляризованном свете, – которые упрощают процесс идентификации дефектов. С практической точки зрения для видеосистем освещенность должна быть минимальной, а для оптических микроскопов необходима возможность ее регулировать.

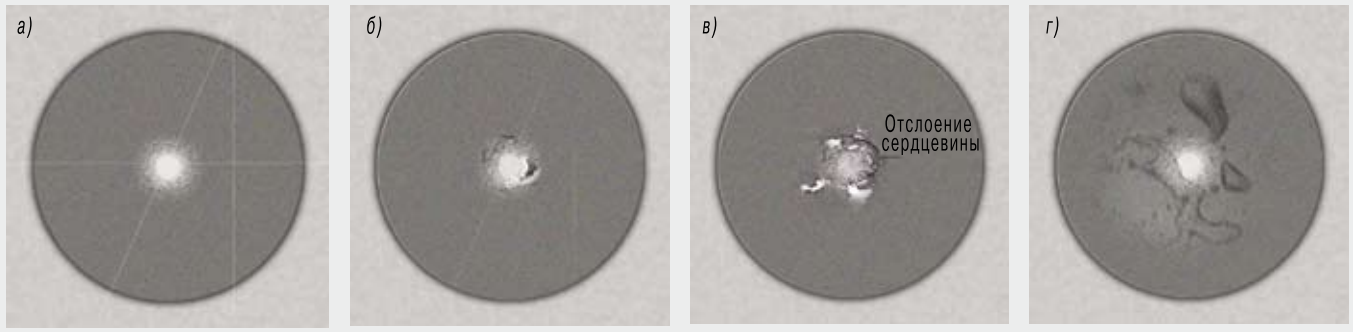
Разрешающая способность системы определяет размер дефектов, которые удается выделить и идентифицировать. Число Аббэ ограничивает разрешение оптического микроскопа на уровне половины длины волны света, используемого для подсветки объекта. Таким образом, для видимого света разрешение будет на уровне 0,25 мкм. С другой стороны, разрешение системы зависит от числовой апертуры и длины волны, а не от коэффициента увеличения. В видеосистемах разрешающая способность напрямую связана с количеством пикселов матрицы используемой камеры.

Типы дефектов

В существующих отраслевых стандартах принято различать несколько типов дефектов поверхности. Один из них – царапины, механические повреждения в виде тонких линий (рис. 1, *а*). Наличие царапин говорит об отклонениях в технологии оконцевания и полировки соединителей и напрямую характеризует качество продукции. В большинстве случаев такие дефекты имеют необратимый характер.

Второй тип дефектов – раковины, выщербины, сколы (рис. 1, *б*). Раковины обычно возникают на поверхности керамического ферула в процессе транспортировки и монтажа оптических компонентов при ударах и контакте с твердыми поверхностями упаковки, серверных шкафов и активного оборудования. Вероятность возникно-

Рис. 1. Торцы ферула с различными типами дефектов: *а* – царапины; *б* – раковины; *в* – отслоение сердцевины; *г* – посторонние включения (капли жидкости)



вения таких дефектов зависит от качества упаковки пассивных компонентов, в которой продукция поставляется от производителя. Сколы характерны для стекла оболочки или сердцевины волокна и говорят о нарушениях технологического режима в производстве компонента (процесс формирования скола волокна). Дефекты могут быть обусловлены и присутствием фиксированных механических частиц: это остатки эпоксидного клея, дефекты полировки керамического ферула.

Еще один тип дефектов – трещины. Наиболее часто они встречаются в системах спектрального уплотнения WDM. Так, из-за разницы в коэффициентах линейного расширения стекла сердцевины и оптической оболочки может происходить отслоение материала при высоких плотностях оптической мощности излучения (рис. 1, *в*).

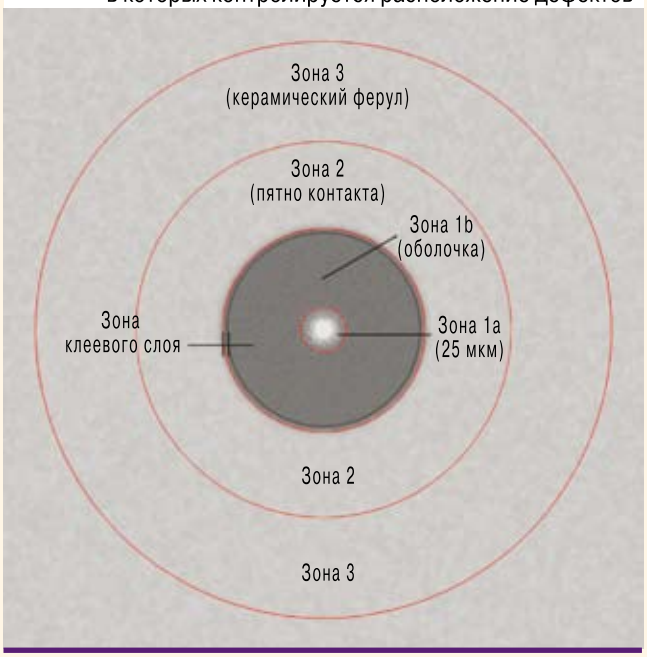
Присутствие посторонних включений – пыли, следов жидкости, органических волокон и т.п. (рис. 1, *г*) – вносит дополнительный вклад в ухудшение вносимых и обратных потерь в соединении.

О чем говорят стандарты

Существует несколько отраслевых стандартов, определяющих требования к состоянию поверхности ферула и наличию дефектов. Большинство документов основываются на одних и тех же результатах исследований. В 2004 г. в рамках iNEMI была сформирована рабочая группа представителей производителей активного и пассивного оборудования (iNEMI – Fibre Optic Signal Performance Project), главной целью которой являлись пересмотр существовавших на тот момент норм и выработка новых рекомендаций.

Одним из нововведений по результатам исследований стало определение зоны 2 (пятно контакта) на поверхности (рис. 2). Диаметр пятна контакта двух соединяемых разъемов зависит от контактного усилия, которое обеспечивается прижимными пружинами разъема, а также упругими свойствами материала ферула и радиусом его полировки. Например, для оптического интерфейса SC значение контактного усилия лежит в диапазоне 4,9–8,8 Н, который определяется жесткостью пружин в разъемах и силой трения соединяемых ферулов о поверхность центрирующей втулки розетки.

Рис. 2. Отраслевые рекомендации определяют зоны, в которых контролируется расположение дефектов



Для типовых разъемов SC диаметр пятна контакта находится в диапазоне 155–185 мкм. Таким образом, чтобы обеспечить гарантированный физический контакт, необходимо ограничить количество и размер дефектов в рассматриваемой области. При верхнем значении контактного усилия на уровне 8,8 Н и радиусе полировки 30 мм предельное значение диаметра пятна контакта составляет 195 мкм. Практическое подтверждение полученных результатов обусловило введение второй зоны, ограниченной диаметром 250 мкм. Сравнение существующих норм различных стандартов проведено в таблице.

Некоторые практические наблюдения

Визуальный контроль состояния торца ферула разъемного соединителя является обязательной частью процесса подключения активного оборудования. В большинстве случаев отрицательный результат контроля бывает вызван тремя причинами: наличие на по-

Нормы различных стандартов

Тип дефекта	Рекомендации	Зона 1a (0–25 мкм)	Зона 1b (25–120 мкм)	Клеевой слой (120–130 мкм)	Зона 2 (130–250 мкм)
Царапины	iNEMI	Недопустимы > 3 мкм	Недопустимы > 3 мкм	Допустимы любые	Допустимы любые
	IPC-8497-1*	Недопустимы	Недопустимы > 3 мкм	Допустимы любые	Допустимы любые
	IEC 61300-3-35**	Недопустимы	Недопустимы > 3 мкм	Допустимы любые	Допустимы любые
Раковины, сколы, выщербины	iNEMI	Недопустимы	Допустимы < 2 мкм, до 5 дефектов 2–5 мкм, недопустимы > 5 мкм	Допустимы любые	Недопустимы >10 мкм
	IPC-8497-1	Недопустимы	Допустимы < 2 мкм, до 5 дефектов от 2–5 мкм, недопустимы > 5 мкм	Допустимы любые	Допустимы любые
	IEC 61300-3-35	Недопустимы	Допустимы < 5 мкм	Допустимы любые	Недопустимы > 10 мкм

* IPC-8497-1 - Cleaning Methods and Contamination Assessment of Optical Assembly; ** IEC 61300-3-35 – Fibre optic cylindrical connector endface visual and automated inspection.

верхности царапин, следов пальцев, частиц пыли. Рассмотрим более подробно первые две.

Царапины на поверхности торца волокна. В общем случае царапины могут располагаться как в пределах сердцевины волокна (зона 1а), так и вне ее. Практические эксперименты в рамках проекта iNEMI показали, что наличие и характер царапин (их ширина, глубина, протяженность) вне сердцевины слабо влияют на уровень прямых и обратных потерь (их влияние сопоставимо с величиной погрешности измерительного прибора).

С другой стороны, царапины в зоне сердцевины могут значительно ухудшить вносимые потери и усилить отражение из-за появления воздушного зазора. Однако, по данным исследований, царапины малой ширины (не более 2 мкм) привносят существенно меньшие потери. Такая зависимость обусловлена механизмом разрушения стекла; как правило, глубина царапин и их ширина примерно одинаковы.

Для однозначного принятия решения о размерах и характере дефекта необходим соответствующий микроскоп. Как указывалось выше, разрешающая способность микроскопа определяется длиной волны света и числовой апертурой. В случае видимого света предел Аббэ равен четверти микрона, и этого совершенно достаточно для оценки характера дефекта. Единственная рекомендация здесь: использовать микроскоп или видеосистему с увеличением не менее 400-кратного. Стандартные микроскопы с 200-кратным увеличением дают пользователю лишь общее представление о состоянии поверхности волокна и, как правило, не имеют градуированной шкалы.

Присутствие органических веществ. Одна из распространенных причин ухудшения характеристик в соединении – тонкий слой органической жидкости на торце разъема. Это могут быть остатки растворителя, жидкости для чистки разъемов или для снятия гидрофобного заполнителя при разделке оптического кабеля.

Практический интерес представляет влияние жировых следов, которые оставляют пальцы человека при контакте с поверхностью ферула в процессе монтажа и обслуживания оборудования. Жир случайным образом распределяется по поверхности и имеет тенденцию перераспределяться между поверхностями двух соединяемых разъемов.

Рис. 3. Прямые (IL) и обратные потери (RL) оптического разъемного соединения в зависимости от загрязнения сердцевины

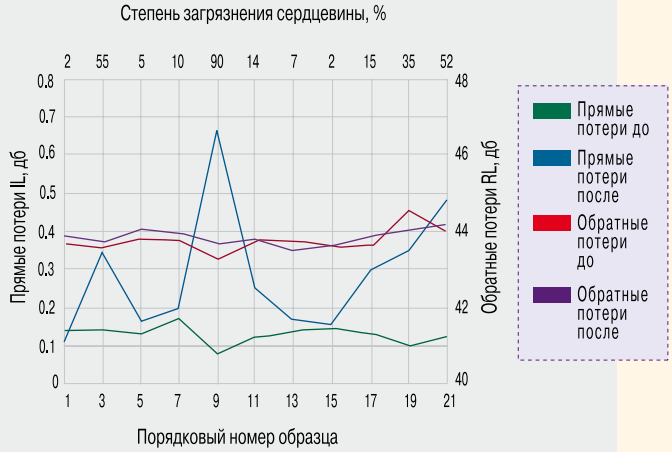


Рис. 4. Присутствие жирных следов пальцев приводит к туннелированию излучения в оптическом интерфейсе MTP/MPO

Измерения прямых и обратных потерь показывают, что достаточно трех последовательных соединений разъемов, чтобы получить одинаковое количество жира на обеих поверхностях. Интересно также, что значения коэффициентов преломления стекла сердцевины волокна (1,4612) и жира (1,4673) очень близки. Поэтому жир можно рассматривать в качестве аналога иммерсионного геля, снижающего отражение от границы раздела двух сред.

Как видно из рис. 3, после загрязнения соединения уровень обратных потерь практически не изменился. Прямые же потери изменяются очень существенно, в разы, так как у жира другие характеристики поглощения и рассеяния света.

Дополнительным негативным эффектом от присутствия органических веществ может стать туннелирование света в многополюсных разъемах типа MTP/MPO (рис. 4). При вводе излучения в волокно номер 1 на торце MT-ферула можно наблюдать излучение из нескольких смежных волокон.

■ ■ ■

Визуальный контроль дефектов на поверхности ферула оптического соединителя – задача сама по себе несложная. Для успеха важно правильно выбрать соответствующее измерительное оборудование с оптическими параметрами, позволяющими достичь желаемого результата.

Идентификация типа дефекта и принятие решения о замене дефектного изделия, например оптического патчкорда, возможны только при условии однозначной интерпретации получаемого изображения. Здесь вопрос цены, как правило, имеет значение.

Безусловно, правила культуры обслуживания разъемных соединителей включают в себя и процедуры чистки разъемов (удаления включений). Здесь нужно запомнить простое правило: не каждая жидкость является чистящей; не всякая чистящая жидкость безопасна для оптического волокна. Таким образом, необходимо с особой тщательностью подходить к выбору оборудования и расходных материалов для обслуживания соединителей, консультируясь при необходимости с поставщиками оборудования и кабельных систем. ИКС

Аспирационные системы для раннего обнаружения возгораний в ЦОДах

Как известно, день простоя дата-центра обходится в десятки, а то и в сотни миллионов долларов. Для непрерывной работы дата-центр должен быть защищен от многих опасностей, в том числе и от пожаров. В крупных американских и европейских ЦОДах для этого активно используют аспирационные системы раннего обнаружения возгораний.

Елена КУРГАШЕВА,
ведущий эксперт компании «АРМО-Системы» по системам пожарной сигнализации

Специфика пожарообнаружения в ЦОДах

Дата-центр – это высокотехнологичное сооружение, потребляющее больше электроэнергии, чем обычный офис. Важное требование к дата-центрам – поддержание определенной температуры воздуха в помещении. Этой цели служит специальная система кондиционирования, с помощью которой создаются внутренние воздушные потоки между стойками и внутри них, обеспечивающие отвод избыточного тепла и комфортную температуру для работы оборудования.

Такая сложная система кондиционирования требует специального подхода к пожарообнаружению. Дело в том, что при наличии сильных воздушных потоков обычные пожарные извещатели для обнаружения дыма или теплового излучения малоэффективны. Дым, подгоняемый воздушными потоками, может не попасть в дымовую камеру извещателя. И если он все же попадает в камеру, то к этому моменту в помещении достигнута предельная концентрация дыма, так что когда срабатывает извещатель, распространение огня уже неизбежно. Поэтому в современных дата-центрах используют активные аспирационные системы пожарной сигнализации.

В настоящее время аспирационные системы пожарной сигнализации выпускают только за рубежом; основные их производители – компании Bosch, Safe Fire Detection, Securiton, System Sensor и Xtralis (ей принадлежат марки оборудования VESDA и Icam, последняя недавно была куплена ею).

Системы данного класса, например, VESDA и Icam от Xtralis, Titanus компании Bosch Security или аспирационные извещатели System Sensor одноименной компании, уже используются во многих странах мира на объектах такого типа, в том числе и в России.

Следует отметить, что в требованиях некоторых международных страховых компаний уже прописывается использование систем раннего обнаружения пожара, в том числе и как средства снижения страховых выплат. А в регламентах крупнейших международных ИТ-компаний система раннего обнаружения пожара является частью системы пожарной безопасности.

Принцип работы

Аспирационные системы – это системы раннего обнаружения пожара. Как правило, они имеют модульную архитектуру, которая позволяет адаптировать систему к конкретным условиям эксплуатации и планировке здания. Основные компоненты такой системы – трубопровод для забора воздуха из контролируемой области и сам извещатель, который можно разместить в любом месте внутри защищаемого помещения или вне его.

В качестве трубопровода обычно используют трубы ПВХ. С помощью переходников, уголков, тройников и других аксессуаров можно создавать гибкие сети трубопроводов для забора воздуха с учетом особенностей каждого отдельно взятого помещения. При этом сам аспирационный извещатель создает вакуум в системе трубопровода, чтобы обеспечить непрерывный забор воздуха из контролируемой области через специально сделанные отверстия. Эти активно получаемые образ-

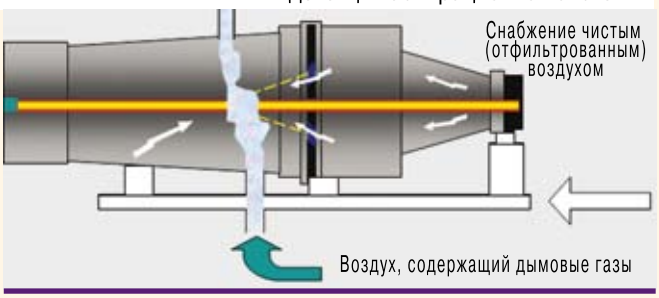
Историческая справка

В 1967 г. американские исследователи Алквист и Чарлсон (Ahlquist & Charlson) впервые создают прибор нефелометр для измерения прозрачности воздуха и степени его загрязнения, позволяющий контролировать содержание углекислого газа на городских улицах. Это устройство было усовершенствовано и выпущено на рынок в США. В 1970 г. австралийское содружество CSIRO использовало нефелометр в исследованиях лесных пожаров. Немногим позже в CSIRO обратился главный департамент почты APO с заказом на изучение проблемы предотвращения пожаров в почтовых службах. Целью исследования было найти наиболее подходящую технологию для защиты от пожаров телефонных станций, компьютерных комнат и кабельных туннелей. Источниками риска на этих объектах были кабели, которые разогревались от электрического тока или от горячих пластин. В этом исследовании CSIRO использовало нефелометры, с помощью которых контролировали степень задымления в вентиляционных каналах. Впоследствии данное исследование дало толчок к разработке высокочувствительного прибора, способного обнаруживать задымление на ранней стадии пожара. Выход усовершенствованной версии этого прибора на рынок стал огромным скачком в развитии систем раннего обнаружения задымления.

цы воздуха проходят через камеру детекции, в которой проверяются на содержание в них частиц дыма. Кроме того, например, в системе VESDA, из пробы воздуха сначала удаляются пыль и загрязнения с помощью встроенного фильтра, а потом проба подается в камеру аспирационного извещателя. Это предотвращает загрязнение оптических поверхностей камеры.

Проба воздуха поступает в калиброванную камеру извещателя, в которой через нее проходит луч лазера. При наличии в воздухе частиц дыма наблюдается рассеивание света внутри камеры, и это немедленно обнаруживается высокочувствительной приемной системой (рис. 1). Затем сигнал обрабатывается и отображается на гистограммном дисплее, пороговых индикаторах срабатывания сигнализации и/или графическом дисплее. Чувствительность извещателя можно регулировать, а поток воздуха непрерывно контролируется на предмет обнаружения повреждений трубопровода.

Рис. 1. Принцип действия камеры детекции аспирационной системы



Аспирационные извещатели условно делят на две категории. Первая – извещатели типа PIB (Point in the box), в которых в качестве камеры детекции используют обычные дымовые датчики повышенной чувствительности, например, ASD-Pro или LASD компании System Sensor с чувствительностью от 0,03 до 3,33%/м. Вторая группа – аспирационные извещатели типа VESDA, Icam или Titanus, которые имеют собственные встроенные камеры детекции дыма с диапазоном чувствительности от 0,005 до 20%/м у VESDA, от 0,001 до 20%/м у Icam и от 0,05 до 10%/м у Titanus. Мы рассмотрим только извещатели второй группы, поскольку именно они имеют наибольший диапазон чувствительности по сравнению с PIB, что позволяет детектировать пожар еще на стадии плавления провода и устанавливать наиболее высокий порог для запуска системы газового пожаротушения помещений дата-центров.

Особенности и преимущества

Классические системы пожарной сигнализации не срабатывают, пока не начнется тление или не появится огонь. На этом этапе возгорания борьба с пожаром уже становится сложным делом. Важнейшее преимущество аспирационных систем заключается в том, что они обнаруживают зарождающийся огонь и обеспечивают раннее оповещение о пожаре. Интеллектуальный процессор камеры детекции дыма анализирует полученные данные и принимает решение о том, соответствуют ли они каким-либо типичным моделям пожара. При этом внешние факторы, которые могут стать причиной ложных срабатываний, подавляются.

Итак, в чем же основные преимущества аспирационных систем?

1. Надежное обнаружение возгорания для раннего предупреждения. Высокочувствительные датчики определяют возгорание на самой ранней его стадии – в фазе пиролиза, еще до распространения видимых частиц дыма (например, когда начинает оплавляться провод или другой электронный элемент оборудования). В большинстве случаев такие системы предотвращают значительный материальный ущерб, поскольку быстро выявляют вышедший из строя элемент, который можно обесточить, не дав зарождающемуся пожару перейти в активную фазу. Кроме того, аспирационные системы позволяют не вводить в действие систему активного (как правило, газового) пожаротушения и экономят средства, необходимые для перезарядки газовых баллонов.

2. Сокращение числа ложных срабатываний. Благодаря интеллектуальной обработке сигнала с датчиков в аспирационных системах подавляются внешние факторы, например, пыль, сквозняки или электрические помехи, которые часто становятся причиной ложных тревог. Это обеспечивает более высокую чувствительность и надежность работы системы даже в помещениях с высокими потолками или экстремальными температурами, а также в условиях загрязненности или высокой влажности.

3. Быстрый монтаж и простое обслуживание. Извещатели можно установить в любом месте как снаружи, так и внутри помещения, чтобы специалистам по обслуживанию было удобнее получить к ним доступ. Аспирационные системы незаметны в помещении, а их обслуживание не требует высокой квалификации. Информация о всех неисправностях, таких как повреждение трубопровода, загрязнение фильтра и т.д., выводится на экран дисплея. Таким образом, персоналу не приходится тратить много времени на выявление неисправности системы, ее можно обслуживать по мере поступления информации.

Основное и принципиальное отличие аспирационных систем от обычных систем с пассивными датчиками дыма – активный забор проб воздуха из коммуникационных и серверных шкафов дата-центра, посредством встроенного вентилятора, работающего по принципу пылесоса. Другим важным отличием является более высокая чувствительность извещателей, что позволяет обнаруживать частицы дыма, невидимые для человеческого глаза, с концентрацией от 0,005%/м у системы VESDA, от 0,001% у Icam или от 0,05 % у Titanus.

Немаловажная особенность – наличие встроенного (как у системы VESDA) и/или внешнего фильтра, где очищается всасываемый воздух. Такие фильтры позволяют эксплуатировать аспирационные системы в сильно загрязненных помещениях без постоянной очистки или замены лазерных камер, что, в свою очередь, увеличивает срок службы системы и сокращает расходы на ее обслуживание.

Области применения

В некоторых случаях применение аспирационных систем приносит ощутимый результат по сравнению с обычными пассивными извещателями. В первую очередь это предприятия и компании, где непрерывность производственных или бизнес-процессов имеет первостепенное значение, а простои недопустимы. Таковы, например, телекоммуникационные системы и серверные финансовых организаций, коммунальные объекты и медицинские стерильные помещения (операционные), энергетические и транспортные системы. Аспирационные системы полезны и тогда, когда необходимо исключить ложное срабатывание системы активного пожаротушения, приводящее к большим затратам времени и средств на восстановление объекта.

Аспирационные системы предпочтительны в помещениях, где обнаружение дыма затруднено, например, при интенсивных воздушных потоках или в высоких атриумных пространствах (торговые центры, спортивные залы, театры, музеи и т.д.). Их используют и в помещениях, где доступ для технического обслуживания невозможен или затруднен; они оптимальны для защиты пространства за подвесным потолком и под фальшполом, лифтовых шахт, производственных зон, воздуховодов, а также тюрем и других мест содержания под стражей. Еще одна сфера применения – в экстремальных условиях окружающей среды: при сильной запыленности, загазованности, влажности, очень высоких или очень низких температурах (например, на электростанциях, бумажных или мебельных фабриках, в автомастерских, шахтах). И наконец, аспирационные системы используют, если важно сохранить дизайн помещения и средства обнаружения задымления требуется скрыть.

Построение аспирационной системы в ЦОДе

Как правило, оборудование дата-центров находится в закрытых шкафах, поэтому наиболее эффективным решением для защиты этих зон является отбор проб из шкафов. В случае аспирационных систем в дата-центрах трубки с всасывающими отверстиями проводят поверх стоек с установленным оборудованием. Гибкая система трубок позволяет отбирать пробы как над шкафами, так и внутри них с помощью капилляров, обеспечивая максимально надежное обнаружение дыма в полностью закрытых шкафах, равно как и в шкафах с верхней вентиляцией (рис. 2).

Активное всасывание воздуха и последующий его анализ на содержание частиц дыма в аспирационной камере дает возможность построить систему таким образом, чтобы потоки воздуха в помещении не влияли на обнаружение задымления. Например, с помощью датчика Icam можно защитить до 15 стоек, проложив в каждую из них отдельную трубку-капилляр, а также обеспечить адресность, определяя место возгорания с точностью до отдельного шкафа. Принцип работы датчика Icam – поочередный забор воздуха из каждой трубки и дальнейший его анализ на содержание частиц дыма в камере детекции.

У системы Titanus есть функция ROOM-IDENT, которая обеспечивает раннее обнаружение возгораний и определение их местонахождения. Один извещатель может контролировать до пяти помещений или пяти стоек при прокладке только одной трубки. Процесс определения источника возгорания системой ROOM-IDENT включает четыре этапа, а результат отображается на извещателе.

Этап 1 (обычный режим): трубопровод используется для забора и оценки образцов воздуха в нескольких помещениях.

Этап 2 (раннее обнаружение возгорания): всасывание и анализ воздуха. При наличии дыма немедленно включается тревожный сигнал для раннего реагирования.

Этап 3 (обратная циркуляция): при включении тревожного сигнала всасывающий вентилятор выключается и включается второй, нагнетательный вентилятор, выдувающий все частицы дыма из трубопровода в противоположном направлении.

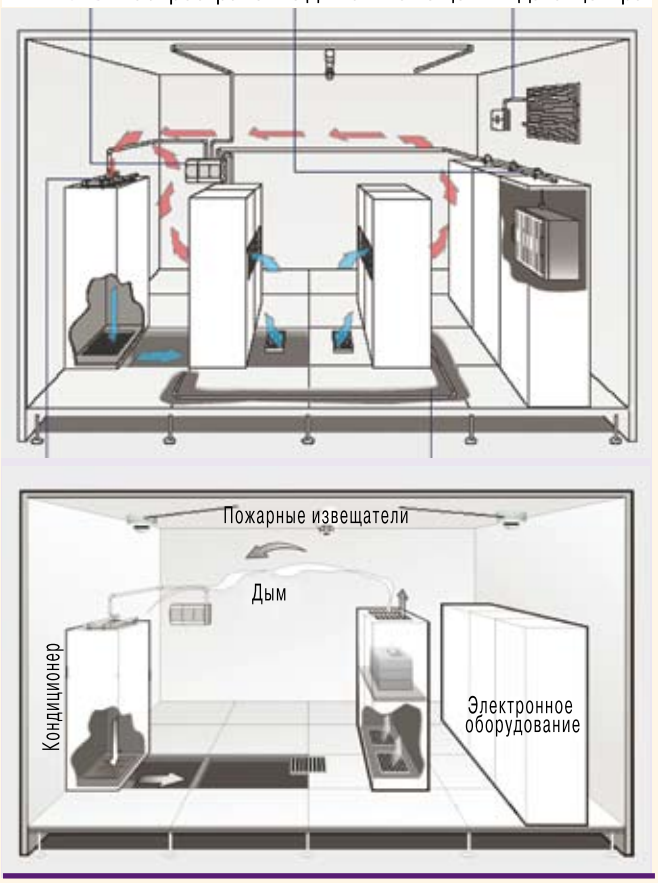
Этап 4 (определение местонахождения): после продувки трубопровода направление движения воздуха снова меняется. На основании замеров времени, которое потребовалось частицам дыма, чтобы достичь модуля детекции, система определяет местонахождение возгорания.

Используя гибкую систему трубопроводов, с помощью одного датчика VESDA можно, например, контролировать пространство не только над стойками, но и за фальшпотолком и фальшполом, а также кабельные лотки, которые есть в любом дата-центре и часто являются источником пожара. Кроме того, извещатели системы VESDA встраиваются в rack-стойку, что экономит место и обеспечивает конструктивную однотипность всего оборудования в дата-центре.

Еще один ключевой момент организации надежной системы пожарообнаружения – забор воздуха непосредственно у решетки приточно-вытяжной вентиляции помещения. Появившийся дым неизбежно попадает в воздушный поток, поэтому установка системы труб с заборными отверстиями на решетке возврата воздуха системы циркуляции обеспечивает моментальное обнаружение зарождающегося пожара на самой ранней стадии.

Рис. 2. Разводка трубопровода в помещениях дата-центров

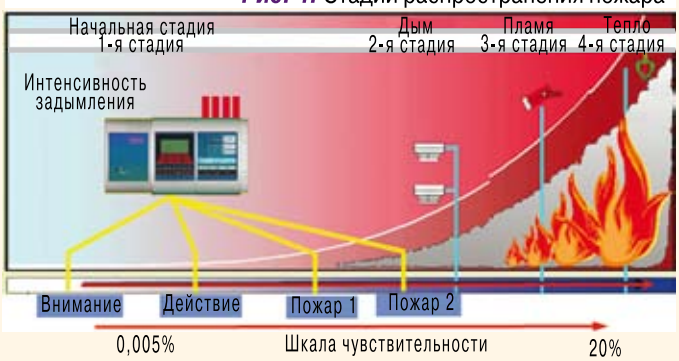
Рис. 3. Распространение дыма в помещениях дата-центра



Забор проб воздуха непосредственно рядом с решеткой вытяжной вентиляции позволяет уловить в воздухе частицы дыма даже в том случае, если создаваемые воздушные потоки миновали все остальные заборные отверстия трубок в помещении. Это связано с тем, что через вытяжную вентиляцию циркулирует весь воздух, содержащийся в помещении, а значит, ни одна частица дыма, содержащаяся в воздухе, не пройдет мимо заборного отверстия (рис. 3).

Возможность установки различных уровней пожарной опасности позволяет запрограммировать систему на соответствующие реакции на разных этапах развития пожара, например, на отключение оборудования систем кондиционирования или запуск систем активного пожаротушения. Например, можно установить несколько порогов предтревоги или самую высокую чувствительность – для определения момента плавления элементов оборудования. При превышении данного порога чувствительности сигнал предтревоги будет передан на пожарный пост, чтобы персонал идентифицировал место плавления и отключил питание оборудования, предотвратив распространение пожара.

Рис. 4. Стадии распространения пожара



Сколько стоит защита от пожара

Стоимость решения для пожарной защиты конкретного дата-центра зависит от объема и площади помещения, а также от числа отдельно защищаемых компонентов систем. В любом случае эта стоимость не превышает 1% от стоимости оборудования, установленного в дата-центре. Например, цена 15-канального извещателя Icam, способного защитить 15 стоек с оборудованием, составляет 10—11 тыс. евро, прибор VESDA VLP, который может защитить до 2000 кв.м., стоит 4—5 тыс. евро, а Titanus защищает до 400 кв.м. и стоит 2000—4000 евро.

Можно также установить среднюю чувствительность, и при этом система будет определять момент сильного задымления помещения, когда сложно найти место или оборудование, являющееся причиной задымления. При превышении данного порога чувствительности можно запрограммировать систему на отключение кондиционеров. Самую низкую чувствительность устанавливают для уровня задымленности помещения, когда предотвратить дальнейшее распространение пожара невозможно без систем активного пожаротушения. При достижении данного порога чувствительности программируется включение системы газового пожаротушения (рис. 4).

Включение систем пожаротушения – это второй этап предотвращения распространения пожара в дата-центре, когда развитие пожара уже невозможно остановить с помощью простых действий: отключив задымившийся сервер, системы кондиционирования и т.д. Для активного тушения пожара применяются, как правило, газовые системы пожаротушения, использующие два принципа организации пожаротушения в дата-центре. Первый – это общее газовое пожаротушение, когда проводится тушение общей площади ЦОДа. Второй – стоечное газовое пожаротушение, когда тушат отдельно взятую стойку. Последний принцип применяется для стоек с оборудованием особого назначения, когда потеря данных обойдется дороже установки и эксплуатации системы пожаротушения. Но это уже тема отдельной статьи.

■ ■ ■

Своевременное обнаружение возгорания в дата-центре может предотвратить потерю оборудования и важнейших данных, а также вынужденные простои, сопряженные с финансовыми и материальными затратами для компании. Вложение средств в надежную систему пожарной сигнализации дата-центров гарантирует организации защиту от будущих расходов на восстановление электронного оборудования и потерянной в пожаре информации. Иногда эти финансовые потери несравненно больше, чем затраты на систему обнаружения возгорания на ранней стадии. ИКС

Нетпоп от Lenovo

Моноблок C200 оснащается процессорами Intel Atom, включая двухъядерные модификации, 18,5-дюймовым дисплеем с соотношением сторон 16:9, встроенным DVD-приводом и акустической системой. Опционально комплектуется видеосистемой NVIDIA ION.

Благодаря встроенной веб-камере, способной работать даже при низкой освещенности, может использоваться для видеоконференций.

Как и другие настольные ПК Lenovo, C200 оснащен системой Lenovo Rescue System. С ее помощью компьютер можно восстановить после программного сбоя либо переписать данные на внешний носитель даже в том случае, если операционная система не загружается. Простой интерфейс системы позволяет вернуть компьютер к жизни даже неопытному пользователю.

Стоимость C200 – от 20 тыс. руб.

Lenovo: (495) 937-3131

Передвижные кондиционеры

серии SmartRack

обеспечивают дополнительное охлаждение электронного оборудования в местах, где мощностей кондиционирования объекта не хватает для обеспечения достаточного охлаждения или они недоступны в нужном месте для компенсации неблагоприятных условий окружающей среды.

Основные достоинства SmartRack:

- охлаждающая способность – 12 000 BTU;
- отсутствуют внешние конденсаторы, радиатор охлаждения или трубопроводы, вследствие чего конструкция не нуждается в обслуживании;
- удаление конденсата происходит вместе с отводимым воздухом, поэтому не требуется опорожнять емкость для воды;
- направленный воздуховод поставляет холодный воздух точно к месту назначения;
- устройство занимает мало места и помещается в тесных пространствах, куда не может быть подведено стационарное кондиционирование;
- отличается простотой установки и работает, не требуя вмешательства;
- экологически безвредный хладагент соответствует мировым нормам по охране окружающей среды;
- в комплекте имеется монтажный набор, предназначенный для отвода горячего воздуха через окно или за фальшпотолок.

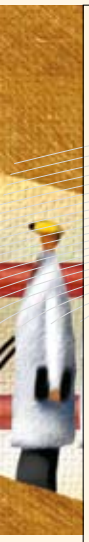
Tripp Lite: (495) 799-5607

Коаксиальные разъемы Spinner MultiFit

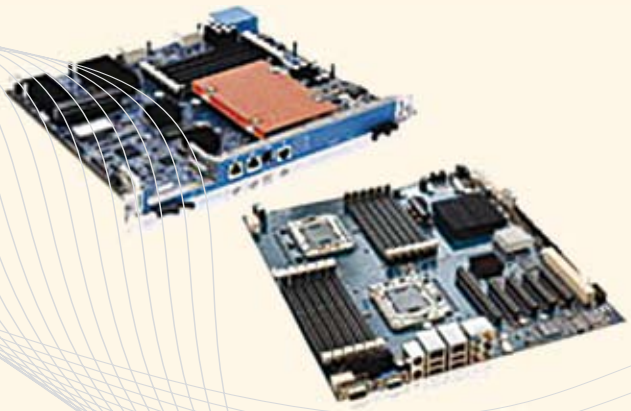
Высокочастотный разъем MultiFit обеспечивает совместимость со всеми ходовыми кабелями 7/8“, отличается небольшой массой и простым монтажом и удовлетворяет высоким требованиям к герметичности. Специальное приспособление в комплекте дает возможность точно

зачистить кабель для монтажа подручными инструментами. При этом тип кабеля не играет роли – с медным или алюминиевым внешним проводником; с гофрированным или гладким внутренним проводником. Разъемы MultiFit подходят для кабелей производителей Acome, Andrew, Draka, Eupen, Hansen, Leoni, LS Cable, RFS, «Цветлит».

ООО «КР Системы»: (495) 728-9099



ATCA- и серверный модули на базе Intel Xeon 5600



Новые версии AdvancedTCA-модуля Kontron AT8050 и серверного модуля Kontron KTC5520 будут выпускаться как с процессорами Intel Xeon 5500, так и с процессорами серии Xeon 5600.

Ключевые отличия процессоров Intel Xeon 5600 от процессоров серии Intel Xeon 5500 – наличие шести ядер вместо четырех, 12 потоков вместо восьми, 32-нм техпроцесс против 45-нм, рост производительности при сохранившемся уровне тепловыделения, память LVDDR3L со сверхнизким энергопотреблением.

AdvancedTCA-модуль AT8050 имеет один сокет для установки четырехъядерного Intel Xeon L5518 или шестиядерного Intel Xeon L5638. Оба варианта совместимы с существующим чипсетом Intel 5520, поддерживают до 36 портов PCI Express 2.0 × 1 и технологию виртуализации прямого ввода-вывода VT-d (Virtualization technology for directed I/O), которая ускоряет обмен данными и уменьшает нагрузку на процессор как в обычном, так и в виртуализированном режиме. Модуль AT8050 обеспечивает лучшее соотношение цены и производительности для оборудования стандарта AdvancedTCA, применяющегося при создании медиасерверов, а также в сетях 3G и LTE EPC (Evolved Packet Core).

Серверный модуль KTC5520, предназначенный для использования в приложениях класса high end, в центрах обработки данных и для облачных вычислений, выполнен в формфакторе SSI EEB и имеет два сокета, поддерживающих процессоры Intel Xeon серий 5500 и 5600. Наряду с оригинальной версией с процессорами Intel Xeon 5500, модуль KTC5520 доступен в модификации с двумя процессорами Intel Xeon L5638, каждый из которых потребляет 80 Вт. Обе модели KTC5520 обеспечивают большую пропускную способность данных и имеют гарантированный семилетний жизненный цикл. KTC5520 допускает удаленное администрирование посредством специального процессора управления (Integrated Management Processor – IMP) с интегрированным видеоконтроллером VGA/2D, контроллером управления платой (Baseboard Management Controller – BMC) и поддержкой технологии KVM/VM (Keyboard, Video, Mouse/Virtual Media). Последняя позволяет обращаться к системе в режиме реального времени по IP-протоколу в любой момент и из любого места и полностью контролировать модуль при помощи клавиатуры, монитора, мыши и виртуальной среды.

«РТСофт»: (495) 742-6828

Устройство обеспечения сетевой безопасности

Система Intrusion Prevention System (IPS), предназначенная для защиты сетевых и/или системных операций от злонамеренных действий, объединяет средства предотвращения вторжений с защитой данных и веб-приложений в едином устройстве. Это устройство поставляется с установленным и сконфигурированным программным обеспечением IBM для обеспечения безопасности.

IPS обеспечивает:

- защиту от атак типа zero-day;
- защиту веб-приложений (благодаря интеграции с решением IBM Security AppScan система IPS может автоматически генерировать специальные политики безопасности для защиты веб-приложений, исходя из уязвимостей, выявленных с использованием AppScan);
- защиту данных на основе мониторинга, осуществляемого с целью пресечения выхода конфиденциальной информации за пределы сети;
- высокую производительность платформы, более чем вдвое превышающую возможности устройств предшествующего поколения;
- удобство использования за счет упрощения развертывания и повседневного управления;
- поддержку IPv6.

IBM: (495) 775-8800

Блог, еще раз блог!

ИКС

Петр ДИДЕНКО

Сколько – не грабёж?

>>>> Мне кажется, что индустрия терминалов оплаты – обдираловка и грабеж не сильно умного населения, которое не понимает, что 1-2-3-4-5 процентов комиссии за операцию – это колоссальные деньги и что ни в коем случае не надо столько платить этим жуликам.

Мое мнение: правительству надо запретить ВСЕ терминалы вот прямо завтра и выдать всем банковские карты. Банкоматов нужно ЧУТЬ побольше, основной акцент делать на internet usage. Детали можно было бы доработать до такого состояния, что в целом идея работала бы. Заодно из тени вывели бы огромные деньги.

Я решил в ходе предстоящей своей поездки в США опросить несколько знакомых (или даже незнакомых) людей о том, как они оплачивают коммунальные услуги, мобильную связь, Интернет и прочие постоянные расходы. Сколько при этом платится комиссии и как люди относятся к терминалам, которые принимают кэш за 1-2-3-4-5 процентов.

Я хотел бы, чтобы вы рассказали мне, за что вы платите через терминалы, какой процент с вас обычно берут и считаете ли вы этот процент приемлемым. Было бы интересно собрать побольше данных.

комментировать

Михаил ЕЛАШКИН

Половинка истины об инновациях

>>>> Колумнист New York Times Томас Фридман, лауреат Пулитцеровской премии и прочая, написал в NYT о том, что корпорации зажрались и спасать их в кризис – это значит выбрасывать деньги, а настоящие преимущества Америке дает именно иммиграция и дух предпринимательства, в высшей форме выраженный в виде стартапов.

По Фридману, проблема Америки в том, что в условиях кризиса сокращаются затраты на высшее образование, происходит ограничение иммиграции, общество отвращает талантливых людей от работы «на правительство» (что-то мне это напоминает...). Томас не говорит, что это уже смертельно, но такие процессы постепенно съедают запас прочности США в техническом лидерстве... Я бы сказал, что очень умеренная критика, но видать, она попала в болевую точку... И по «нарушителю конвенции» нанес залп из главного калибра корпоративных линкоров не менее уважаемый Энди Гроув, который сам вытаскивал Intel на вершину корпоративного Олимпа с уровня маленькой компании. Главный его тезис:

«Фридман ошибается. Стартапы – вещь замечательная, но сами по себе они не могут повысить занятость в технологическом секторе. Не менее важно то, что следует за мифическим моментом изобретения в гараже: процесс превращения опытного образца в продукт массового производства. На этом этапе компании обычно начинают увеличивать масштабы производства. Они думают, как сократить его стоимость, работают над дизайном, строят фабрики и тысячами нанимают новых сотрудников. Наращивание объемов производства – сложная задача, но без него инновациям грош цена.»

Это правда. И это сильный аргумент – действительно сама по себе культура стартапов не гарантирует превращения идеи или изобретения в заводские корпуса, рабочие места и реальную экономику. Для нас, экс-жителей СССР это очевидно: сколько изобретений, сделанных в комнате П-65 в подвале (наш ответ их гаражам) Химфака МГУ на моих глазах, навсегда осталось в пыльном шкафу.

PS Ну, а нам-то что делать? Как в СССР – мечтать о том, чтобы дожить до их загнивания! Для начала научиться делать стартапы и развивать технологии, пусть не для наших заводов. А там посмотрим, как в Америке дела, и пойдем по проверенному пути. Когда доживем...

комментировать

VSATman

«Инмарсат» не хочет отвечать за базар

>>>> Орбитальные позиции и частоты на орбитах – это общее достояние человечества. Дабы его распределить, есть МСЭ, он же ITU. Членами МСЭ являются национальные администрации связи (и делегированные ими). Распределяют частоты и орбиты там по принципу: кто первый встал, того и тапки. А так как частоты – дефицит, то некоторые особо прыткие столбят места на будущее, вдруг потом или сам построю, или торгану соседу. Соответственно МСЭ с такими "бумажными" спутниками борется.

Вот на этом поймали и такого уважаемого оператора, как «Инмарсат», который от имени Супер-Державы Каймановы Острова застолбил в эпоху расцвета проектов типа «Иридиум» и «Глобалстар» место для своей системы подвижной спутниковой связи. Но если первые два успели кинуть инвесторов по-взрослому, тяжеловесный «Инмарсат» пока ворочался, стало ясно, что эти системы убиты сотовыми операторами на корню, и ничего строить он не стал. А заявочка-то на сеть и частоты в МСЭ остались. Теперь подавший ее национальный регулятор ОфКом, как истинный джентльмен, который попался на удочку коммерсантов-проходимцев и запятнал этим свою репутацию в МСЭ, хочет заявочку аннулировать, ибо обещанных в 2001 году спутников на орбите нет.

«Инмарсат», как ни странно, упирается, но все равно проигрывает.

комментировать

Реклама в номере

АЛЮДЕКО-К
Тел./факс: (4942) 31-1733
E-mail: sales5@aludeko.ru
www.aludeko.ru . . . . . с. 15

ГЛОБАЛ-ТЕЛЕПОРТ
Тел.: (495) 647-7777
Факс: (495) 647-7733
E-mail: info_gt-port@synterra.ru
www.globalteleport.ru . . . . с. 12

ИНФОРМЗАЩИТА
Тел./факс: (495) 980-2345
E-mail: market@infosec.ru
www.infosec.ru . . . . . с. 72-73

ИНФОСИСТЕМЫ ДЖЕТ
Тел.: (495) 411-7601
Факс: (495) 411-7602
E-mail: info@jet.msk.su
www.jet.msk.su . . . . . с. 68-69

МГТС
Тел.: (495) 636-0636
Факс: (495) 950-0618
E-mail: mgts@mgts.ru
www.mgts.ru . . . . . 4-я обл.

РОСТЕЛЕКОМ
Тел.: (499) 972-8283
Факс: (499) 972-8222
E-mail: info@rt.ru
www.rt.ru . . . . . с. 11

РТКОММ
Тел.: (495) 645-0170
Факс: (495) 645-0171
E-mail: info@rtcomm.ru
www.rtcomm.ru . . . . . с. 85

РУССКИЕ БАШНИ
Тел./факс: (495) 967-3232
E-mail: info@rtowers.ru
www.rtowers.ru . . . . . с. 56-57

СВЯЗЬСТРОЙДЕТАЛЬ
Тел.: (495) 786-3434
Факс: (495) 786-3432
E-mail: mail@ssd.ru
www.ssd.ru . . . . . с. 13

ЦЕНТРТЕЛЕКОМ
Тел.: (495) 793-2424
Факс: (495) 650-3007
E-mail: vip@centertelecom.ru
www.centertelecom.ru . . с. 2, 4, 23

ALADDIN
Тел.: (495) 223-0001
Факс: (495) 646-0882
E-mail: esafe@aladdin.ru
www.aladdin.ru . . . . . с. 37

ALCATEL-LUCENT
Тел.: (495) 937-0900
Факс: (495) 937-0908
www.alcatel-lucent.com . . 2-я обл.

APC BY SCHNEIDER ELECTRIC
Тел.: (495) 916-7166
Факс: (495) 620-9180
E-mail: apcrus@apc.com
www.apc.ru . . . . . с. 83

DEPO COMPUTERS
Тел.: (495) 969-2222
Факс: (495) 969-2229
E-mail: sales@depo.ru
www.depocomputers.ru . . . с. 79

ISKRA SISTEMI
Тел.: (+386) 151-31000
Факс: (+386) 151-11532
www.iskrasistemi.si/ru. . . . с. 20

LANDATA-EATON
Тел.: (495) 925-7620
Факс: (495) 925-7621
E-mail: info@landata.ru
www.landata.ru . . . . . с. 77

LENOVO
Тел.: (495) 663-8260
Факс: (495) 663-8261
www.lenovo.com/ru . . . . . с. 3

PANASONIC
Тел.: (495) 739-3443
E-mail: office@panasonic.ru
www.panasonic.ru . . . . . с. 19

RITTAL
Тел.: (495) 775-0230
Факс: (495) 775-0239
E-mail:info@rittal.ru
www.rittal.ru . . . . . с. 62-63

STONESOFT
Тел.: (495) 787-9936
www.stonesoft.com . . . . . с. 41

UNITED ELEMENTS
Тел./факс: (495) 790-7434
E-mail: center@uelements.com
www.uel.ru . . . . . с. 17

VERIMATRIX
Тел.: (926) 525-7624
www.verimatrix.com . . . . . с. 74

Указатель фирм

Учредители журнала «ИнформКурьер-Связь»:

ЗАО Информационное агентство «ИнформКурьер-Связь»:
127273, Москва, Сигнальный проезд, д. 39, подъезд 2, офис 212; тел.: (495) 981-2936, 981-2937.

ЗАО «ИКС-холдинг»:
127254, Москва,
Огородный пр-д, д. 5, стр. 3;
тел.: (495) 785-1490, 229-4978.

МНТОРЭС им. А.С. Попова:
107031, Москва, ул. Рождественка, д. 6/9/20, стр. 1;
тел.: (495) 921-1616.